ISACA.CRISC.v2026-06-17.q895

Exam Code:	CRISC
Exam Name:	Certified in Risk and Information Systems Control
Certification Provider:	ISACA
Free Question Number:	895
Version:	v2026-06-17
# of views:	118
# of Questions views:	11290
https://www.freecram.net/torrent/ISACA.CRISC.v2026-06-17.q895.html	

NEW QUESTION: 1
Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:
A. minimize the number of risk scenarios for risk assessment.
B. aggregate risk scenarios identified across different business units.
C. build a threat profile of the organization for management review.
D. provide a current reference to stakeholders for risk-based decisions.
Answer: (SHOW ANSWER)
A risk register is a document that records and tracks the information and status of the identified risks and their responses. It includes the risk description, category, source, cause, impact, probability, priority, response, owner, action plan, status, etc.
Periodically reviewing and updating a risk register with details on identified risk factors primarily helps to provide a current reference to stakeholders for risk-based decisions, which are the decisions that are made based on the consideration and evaluation of the risks and their responses. Providing a current reference to stakeholders for risk-based decisions helps to ensure that the decisions are consistent, appropriate, and proportional to the level and nature of the risks, and that they support the organization's objectives and values.
It also helps to optimize the balance between risk and return, and to create and protect value for the organization and its stakeholders.
The other options are not the primary benefits of periodically reviewing and updating a risk register with details on identified risk factors, because they do not address the main purpose and benefit of a risk register, which is to provide a current reference to stakeholders for risk-based decisions.
Minimizing the number of risk scenarios for risk assessment means reducing the scope and depth of risk analysis and reporting, and impairing the organization's ability to identify and respond to emerging or changing risks. Periodically reviewing and updating a risk register with details onidentified risk factors does not necessarily minimize the number of risk scenarios for risk assessment, and it may not be a desirable or beneficial outcome for the organization.

Aggregating risk scenarios identified across different business units means combining or consolidating the risks that are identified by different parts or functions of the organization, and creating a holistic or integrated view of the organization's risk profile. Periodically reviewing and updating a risk register with details on identified risk factors does not necessarily aggregate risk scenarios identified across different business units, and it may not be a sufficient or effective way to achieve a holistic or integrated view of the organization's risk profile.
Building a threat profile of the organization for management review means creating or developing a summary or representation of the potential threats or sources of harm that may affect the organization's objectives and operations, and presenting or reporting it to the senior management for their awareness and approval. Periodically reviewing and updating a risk register with details on identified risk factors does not necessarily build a threat profile of the organization for management review, and it may not be a comprehensive or reliable way to create or develop a summary or representation of the potential threats or sources of harm that may affect the organization. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-
59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 172 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 2
Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?
A. Ensuring availability of resources for log analysis
B. Implementing log analysis tools to automate controls
C. Ensuring the control is proportional to the risk
D. Building correlations between logs collected from different sources
Answer: (SHOW ANSWER)
The primary consideration when implementing controls for monitoring user activity logs is ensuring that the control is proportional to the risk, because this helps to optimize the balance between the benefits and costs of the control, and to avoid over- or under-controlling the risk. User activity logs are records of the actions or events performed by users on IT systems, networks, or resources, such as accessing, modifying, or transferring data or files. Monitoring user activity logs can help to detect and prevent potential threats, such as unauthorized access, data leakage, or malicious activity, and to support the investigation and remediation of incidents. However, monitoring user activity logs also involves certain costs and challenges, such as collecting, storing, analyzing, and reporting large amounts of log data, ensuring the accuracy, completeness, and timeliness of the log data, protecting the privacy and security of the log data, and complying with the relevant laws and regulations. Therefore, when implementing controls for monitoring user activity logs, the organization should consider the level and impact of the risk that the control is intended to address, and the value and effectiveness of the control in reducing the risk exposure and impact. The organization should also consider the costs and feasibility of implementing and maintaining the control, and the potential negative consequences or side effects of the control, such as performance degradation, user dissatisfaction, or legal liability. By ensuring that the control is proportional to the risk, the organization can achieve the optimal level

of risk management, and avoid wasting resources or creating new risks. References = Risk IT Framework, ISACA, 2022, p. 151

NEW QUESTION: 3
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?
A. The organization's knowledge
B. Ease of implementation
C. The organization's culture
D. industry-leading security tools
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, the organization's culture is the most critical element to maximize the potential for a successful security implementation, because it influences the behavior, attitude, and perception of the stakeholders towards security. The organization's culture includes the values, beliefs, norms, and practices that are shared by the members of the organization. A positive and supportive culture can foster the awareness, commitment, and collaboration of the stakeholders in achieving the security objectives and complying with the security policies and standards. The other options are not the most critical elements, as they are less influential or less challenging than the organization's culture. The organization's knowledge is the collective understanding and expertise of the organization regardingsecurity, which can be enhanced through training and education. Ease of implementation is the degree of difficulty and complexity of implementing security, which can be reduced by using appropriate methods and tools. Industry-leading security tools are the best-in-class solutions and technologies that can provide effective and efficient security, which can be acquired through market research and evaluation. References = CRISC Review Manual, 7th Edition, Chapter 1, Section 1.3.1, page 32.

NEW QUESTION: 4
Which of the following is the BEST approach when a risk treatment plan cannot be completed on time?
A. Replace the action owner with a more experienced individual.
B. Implement compensating controls until the preferred action can be completed.
C. Change the risk response strategy of the relevant risk to risk avoidance.
D. Develop additional key risk indicators (KRIs) until the preferred action can be completed.
Answer: (SHOW ANSWER)
*A risk treatment plan is a document that describes the actions and resources needed to implement the chosen risk response strategy for each identified risk1. A risk response strategy is the way an organization decides to address a risk, such as avoiding, accepting, mitigating, or transferring it2.
*Sometimes, a risk treatment plan may not be completed on time due to various reasons, such as delays, resource constraints, technical issues, or changes in the risk environment. In such cases, the best approach is to implement compensating controls until the preferred action can be completed3.
*Compensating controls are alternative or additional controls that provide a similar level of assurance or protection as the original controls, when the latter are not feasible or sufficient3. Compensating controls can

help to reduce the residual risk or maintain the risk within the acceptable level until the risk treatment plan is fully executed3.
*For example, if the risk treatment plan involves installing a firewall to protect the network from external threats, but the firewall is not available or compatible with the current system, a compensating control could be to use encryption, authentication, or monitoring tools to secure the network traffic until the firewall is installed3.
*Implementing compensating controls is better than the other options because it allows the organization to continue with the risk treatment plan while maintaining an adequate level of security and compliance. The other options are not advisable for the following reasons:
oReplacing the action owner with a more experienced individual (option A) may not solve the problem if the issue is not related to the action owner's competence or performance. Moreover, replacing the action owner may cause disruption, confusion, or conflict in the risk management process.
oChanging the risk response strategy of the relevant risk to risk avoidance (option C) may not be possible or desirable if the risk is associated with a critical or beneficial activity or process. Risk avoidance means eliminating the source of the risk or discontinuing the activity that causes the risk2. This may result in losing opportunities, benefits, or value for the organization.
oDeveloping additional key risk indicators (KRIs) until the preferred action can be completed (option D) may not be effective or efficient if the existing KRIs are already sufficient to monitor and measure the risk. KRIs are metrics or data points that provide early warning signals or information about the level or trend of a risk456. Developing additional KRIs may not reduce the risk or improve the risk treatment plan, but may increase the complexity and cost of the risk management process.
References =
*Key Risk Indicators: Examples & Definitions - SolveXia
*Key Risk Indicators: A Practical Guide | SafetyCulture
*Complete Guide to Key Risk Indicators - RiskOptics
*Risk Response Plan in Project Management: Key Strategies & Tips
*Risk response strategies: mitigation, transfer, avoidance, acceptance - Twproject: project management software,resource management, time tracking, planning, Gantt, kanban
*Risk Response Strategies: A Guide to Navigating Uncertainty - Teamly
*Compensating Controls | Audit and Compliance | Pathlock

NEW QUESTION: 5
Who should be responsible (of evaluating the residual risk after a compensating control has been
A. Compliance manager
B. Risk owner
C. Control owner
D. Risk practitioner
Answer: (SHOW ANSWER)
The control owner should be responsible for evaluating the residual risk after a compensating control has been implemented. A compensating control is a control that provides an alternative or additional measure of protection when the primary or preferred control is not feasible or effective. A residual risk is the risk that

remains after the risk response or mitigation has been applied. The control owner is the person who has the authority and responsibility for designing, implementing, and monitoring the controls that enforce the policy. The control owner can assess the impact and effectiveness of the compensating control on the residual risk, and report the results and recommendations to the risk owner or the risk practitioner. The other options are not as responsible as the control owner, as they are related to the compliance, ownership, or management of the risk, not the evaluation of the control. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.4: Key Control Indicators, page 211.

NEW QUESTION: 6
Which of the following is the MOST important factor to consider when determining whether to approve a policy exception request?
A. Volume of exceptions
B. Lack of technical resources
C. Cost of noncompliance
D. Time required to implement controls
Answer: (SHOW ANSWER)
Noncompliance cost reflects the impact or penalties from deviating from policies. Per ISACA governance best practices, exceptions should only be granted when this cost is understood and deemed acceptable relative to business needs.

NEW QUESTION: 7
If preventive controls cannot be Implemented due to technology limitations, which of the following should be done FIRST to reduce risk7
A. Evaluate alternative controls.
B. Redefine the business process to reduce the risk.
C. Develop a plan to upgrade technology.
D. Define a process for monitoring risk.
Answer: (SHOW ANSWER)
If preventive controls cannot be implemented due to technology limitations, the first step to reduce risk is to evaluate alternative controls. Alternative controls are those that can achieve the same or similar objectives as the original preventive controls, but using different methods or technologies. For example, if a firewall cannot be installed due to hardware compatibility issues, an alternative control could be a network segmentation or a proxy server. Evaluating alternative controls requires assessing their feasibility, effectiveness, efficiency, and cost-benefit. Redefining the business process, developing a plan to upgrade technology, and defining a process for monitoring risk are also possible actions to reduce risk, but they are not the first step, and they may not be feasible or desirable in some situations. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.1, page 4-23.

NEW QUESTION: 8
A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data quality
B. Maintenance costs
C. Data redundancy
D. System integration
Answer: (SHOW ANSWER)
The greatest concern for the risk practitioner when a big data project has resulted in the creation of an application used to support important investment decisions is the data quality. Data quality is the degree to which the data is accurate, complete, consistent, reliable, relevant, and timely. Data quality is essential for the success of any big data project, as it affects the validity and reliability of the analysis and the outcomes. Poor data quality could lead to erroneous or misleading results, which could have negative consequences for the investment decisions and the organization's performance and reputation. The other options are not as concerning as the data quality, although they may also pose some challenges or risks for the big data project.
Maintenance costs, data redundancy, and system integration are all factors that could affect the efficiency and effectiveness of the big data project, but they do not directly affect the accuracy and reliability of the analysis and the outcomes. References = Risk and Information Systems Control Study Manual, Chapter 3, Section
3.3.1, page 3-20.

NEW QUESTION: 9
Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?
A. Cost versus benefit of additional mitigating controls
B. Annualized loss expectancy (ALE) for the system
C. Frequency of business impact
D. Cost of the Information control system
Answer: A (LEAVE A REPLY)
Residual risk is the risk that remains after security controls have been implemented on a system. Residual risk can be accepted, transferred, avoided, or further mitigated. The most important consideration when deciding whether to accept residual risk is the cost versus benefit of additional mitigating controls. This means comparing the potential impact of the residual risk with the cost and effectiveness of implementing more controls to reduce it. If the cost of additional controls outweighs the benefit of reducing the residual risk, then it may be acceptable to accept the residual risk. However, if the benefit of additional controls exceeds the cost, then it may be advisable to implement more controls to lower the residual risk to an acceptable level. References = Risk and Information Systems Control Study Manual, Chapter 3: Risk Response and Mitigation, Section 3.4: Risk Response Selection, p. 156-157.

NEW QUESTION: 10
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?
Freecram.net
A. AI requires entirely new risk management processes.

B. AI potentially introduces new types of risk.
C. AI will result in changes to business processes.
D. Third-party AI solutions increase regulatory obligations.
Answer: (SHOW ANSWER)
Artificial intelligence (AI) solutions can offer significant benefits to an organization, such as improved efficiency, accuracy, and innovation. However, AI also poses new challenges and risks that need to be considered and addressed by senior management. Some of these risks include:
Ethical and social risks: AI solutions may have unintended or undesirable impacts on human values, rights, and behaviors, such as privacy, fairness, accountability, and transparency. For example, AI systems may exhibit bias, discrimination, or manipulation, or may infringe on personal data or autonomy.
Technical and operational risks: AI solutions may have vulnerabilities, errors, or failures that affect their performance, reliability, or security. For example, AI systems may be subject to hacking, tampering, or misuse, or may malfunction or produce inaccurate or harmful outcomes.
Legal and regulatory risks: AI solutions may have unclear or conflicting legal or regulatory implications or obligations, such as liability, compliance, or governance. For example, AI systems may raise questions about ownership, responsibility, or accountability, or may violate existing laws or regulations, or create new ones.
Therefore, a risk practitioner should communicate to senior management that AI potentially introduces new types of risk that need to be identified, assessed, and managed in alignment with the organization's objectives, values, and risk appetite. References = ISACA CRISC Review Manual, 7th Edition, Chapter 3, Section 3.2.2, page 113.

NEW QUESTION: 11
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?
A. Piloting courses with focus groups
B. Using reputable third-party training programs
C. Reviewing content with senior management
D. Creating modules for targeted audiences
Answer: (SHOW ANSWER)
The best approach to ensure the effectiveness of risk awareness training is to create modules for targeted audiences. This means that the risk awareness training should be customized and tailored to the specific needs, roles, and responsibilities of different groups of staff, such as business owners, process owners, IT staff, or external parties. Creating modules for targeted audiences helps to ensure that the risk awareness training is relevant, engaging, and applicable to the participants, and that it covers the appropriate level of detail and complexity. It also helps to enhance the learning outcomes and retention of the risk awareness training, and to foster a culture of risk awareness and responsibility within the enterprise. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.4.1, page 2491

NEW QUESTION: 12
Which of the following should be the PRIMARY basis for prioritizing risk responses?
A. The impact of the risk
B. The replacement cost of the business asset

C. The cost of risk mitigation controls
D. The classification of the business asset
Answer: (SHOW ANSWER)
The primary basis for prioritizing risk responses is the impact of the risk. The impact of the risk is the consequence or effect of the risk on the organization's objectives or operations, such as financial loss, reputational damage, operational disruption, or legal liability. The impact of the risk is one of the key dimensions of risk analysis, along with the likelihood of the risk. The impact of the risk helps to determine the severity and priority of the risk, and to select the most appropriate and effective risk response. The impact of the risk also helps to evaluate the cost-benefit and trade-off of the risk response, and to measure the residual risk and the risk performance. The other options are not the primary basis for prioritizing risk responses, although they may be considered or influenced by the impact of the risk. The replacement cost of the business asset, the cost of risk mitigation controls, and the classification of the business asset are all factors that could affect the value or importance of the business asset, but they do not necessarily reflect the impact of the risk on the business asset or the organization. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.1, page 4-25.

NEW QUESTION: 13
Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?
A. Identification of controls gaps that may lead to noncompliance
B. Prioritization of risk action plans across departments
C. Early detection of emerging threats
D. Accurate measurement of loss impact
Answer: (SHOW ANSWER)
A primary benefit of engaging the risk owner during the risk assessment process is prioritization of risk action plans across departments, because this helps to ensure that the most critical and relevant risks are addressed first, and that the resources and efforts are allocated and coordinated efficiently and effectively. A risk owner is the person or group who is responsible for the day-to-day management and mitigation of a specific risk, and who has the authority and accountability to make risk-related decisions. A risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization's objectives, performance, or value. A risk action plan is the set of actions and tasks that are designed and implemented to reduce the likelihood and impact of a risk, or to exploit the opportunities that a risk may create. By engaging the risk owner during the risk assessment process, the organization can benefit from the following advantages:
* The risk owner can provide valuable input and feedback on the risk identification, analysis, and evaluation, based on their knowledge, experience, and perspective of the risk and its context.
* The risk owner can help to develop and implement the risk action plan, based on their understanding of the risk objectives, expectations, and outcomes, and their ability to influence and control the risk factors and sources.
* The risk owner can help to prioritize the risk action plan, based on their assessment of the risk severity, urgency, and importance, and their consideration of the costs, benefits, and feasibility of the risk actions.

* The risk owner can help to coordinate the risk action plan across departments, by communicating and collaborating with other risk owners, stakeholders, and resources, and by aligning and integrating the risk actions with the organization's strategy, processes, and culture. References = Risk Owners - What Do They Do1

NEW QUESTION: 14
Which of the following can be interpreted from a single data point on a risk heat map?
A. Risk tolerance
B. Risk magnitude
C. Risk response
D. Risk appetite
Answer: (SHOW ANSWER)
A risk heat map is a kind of risk matrix where risks are ranked based on their potential impact and their likelihood of occurring, which allows you to prioritize the risks that pose the greatest threat. The severity of each risk is indicated by color, usually green for low risk, red for high risk, and yellow for medium risk. Therefore, from a single data point on a risk heat map, one can interpret the risk magnitude, which is the product of impact and likelihood. The other options are not directly related to a single data point on a risk heat map, but rather to the overall risk management strategy and context. References = Risk Assessment and Analysis Methods: Qualitative and Quantitative; What Is a Risk Heat Map, and How Can It Help Your Risk Management Strategy; CRISC Certified in Risk and Information Systems Control - Question599

NEW QUESTION: 15
Who is PRIMARILY accountable for identifying risk on a daily basis and ensuring adherence to the organization's policies?
A. Second line of defense
B. Line of defense subject matter experts
C. Third line of defense
D. First line of defense
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following is MOST important when creating a program to reduce ethical risk?
A. Obtaining senior management commitment
B. Defining strict policies
C. Developing an organizational communication plan
D. Conducting a gap analysis
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
An organization has experienced a cyber-attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?
A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact
D. Enterprise risk management (ERM) team
Answer: (SHOW ANSWER)
Risk owners based on risk impact are the most important stakeholders to include in the cyber response team, as they are responsible for the business outcomes affected by the cyber attack and can decide on the appropriate response actions. The other options are not the most important stakeholders to include in the cyber response team, although they may be involved in the process.

NEW QUESTION: 18
To drive effective risk management, it is MOST important that an organization's policy framework is:
A. Approved by relevant stakeholders.
B. Aligned to the functional business structure.
C. Included in employee onboarding materials.
D. Mapped to an industry-standard framework.
Answer: B (LEAVE A REPLY)
Policies must reflect the actual structure and processes of the business to be enforceable and effective. Alignment ensures that policies are understood, applicable, and tailored to how the business operates.
Reference:CRISC Manual - Domain 1, Slide 113-115

NEW QUESTION: 19
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?
A. Conduct a comprehensive review of access management processes.
B. Declare a security incident and engage the incident response team.
C. Conduct a comprehensive awareness session for system administrators.
D. Evaluate system administrators' technical skills to identify if training is required.
Answer: (SHOW ANSWER)

The best way to prevent future occurrences of active network accounts belonging to former employees is to conduct a comprehensive review of access management processes. This review should include verifying that the access rights of all employees are updated regularly, especially when they change roles or leave the organization. The review should also ensure that there are clear policies and procedures for granting, modifying, and revoking access rights, and that these are followed consistently and documented properly. The review should also identify and address any gaps or weaknesses in the access management processes that could lead to unauthorized or inappropriate access. By conducting a comprehensive review of access management processes, the organization can improve its security posture and reduce the risk of data breaches or misuse of resources. References = IT audit: The ultimate guide [with checklist] | Zapier, IT auditing and controls - planning the IT audit [updated 2021]

NEW QUESTION: 20

Which of the following is the PRIMARY objective of aggregating the impact of IT risk scenarios and reflecting the results in the enterprise risk register?

Freecram.net

A. To ensure IT risk appetite is communicated across the organization
B. To ensure IT risk impact can be compared to the IT risk appetite
C. To ensure IT risk ownership is assigned at the appropriate organizational level
D. To ensure IT risk scenarios are consistently assessed within the organization
Answer: (SHOW ANSWER)
The primary objective of aggregating the impact of IT risk scenarios and reflecting the results in the enterprise risk register is to ensure IT risk impact can be compared to the IT risk appetite, as it enables the organization to measure and evaluate the overall level and exposure of the IT risk, and to align and prioritize the IT risk response and strategy with the organizational objectives and regulations. The other options are not the primary objectives, as they are more related to the communication, assignment, or assessment of the IT risk scenarios, respectively, rather than the aggregation or reflection of the IT risk scenarios. References = CRISC Review Manual, 7th Edition, page 109.

NEW QUESTION: 21
Which of the following is the MOST important component of effective security incident response?
A. Network time protocol synchronization
B. Identification of attack sources
C. Early detection of breaches
D. A documented communications plan
Answer: (SHOW ANSWER)
The most important component of effective security incident response is a documented communications plan.
A communications plan defines the roles and responsibilities, channels and methods, frequency and timing, and content and format of the communications that take place during and after a security incident. A communications plan helps to ensure that the relevant stakeholders are informed and updated about the incident status and outcome, and that the incident response activities are coordinated and consistent. A communications plan also helps to manage the expectations and perceptions of the stakeholders, and to

maintain the trust and reputation of the enterprise. Network time protocol synchronization, identification of attack sources, and early detection of breaches are also important components of effective security incident response, but they are not as important as a documented communications plan. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.1.2, page 1931
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 660.

NEW QUESTION: 22
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?
A. Facilitating risk-aware decision making by stakeholders
B. Demonstrating management commitment to mitigate risk
C. Closing audit findings on a timely basis
D. Ensuring compliance to industry standards
Answer: (SHOW ANSWER)
A vulnerability management process is a process that identifies, analyzes, prioritizes, and remediates the vulnerabilities in the IT systems and applications. The effectiveness of a vulnerability management process can be measured by the key performance indicators (KPIs) that reflect the achievement of the process objectives and the alignment with the enterprise's risk appetite and tolerance. The best KPI to measure the effectiveness of a vulnerability management process is the percentage of vulnerabilities remediated within the agreed service level. This KPI indicates how well the process is able to address the vulnerabilities in a timely and efficient manner, and reduce the exposure and impact of the risks associated with the vulnerabilities. The other options are not as good as the percentage of vulnerabilities remediated within the agreed service level, as they may not reflect the quality or timeliness of the remediation actions, or the alignment with the enterprise's risk appetite and tolerance. References = Risk and Information Systems Control Study Manual,
7th Edition, Chapter 4, Section 4.3.2.1, pp. 171-172.

NEW QUESTION: 23
Which of the following is the MOST important metric to monitor the performance of the change management process?
A. Percentage of changes having separation of duties in code deployment
B. Percentage of changes having completed post-implementation verification
C. Percentage of changes having user acceptance testing (UAT) sign-off
D. Percentage of changes having to invoke the rollback plan
Answer: (SHOW ANSWER)
Post-implementation verification ensures that changes achieve the desired outcomes without causing unintended issues. It validates the success of change deployment and minimizes operational disruption, making it the most direct indicator of change management effectiveness.
Reference:CRISC Manual - Domain 4, Slide 430-432

NEW QUESTION: 24
Which of the following BEST supports the integration of IT risk management into an organization's strategic planning?
A. Clearly defined organizational goals and objectives
B. Incentive plans that reward employees based on IT risk metrics
C. Regular organization-wide risk awareness training
D. A comprehensive and documented IT risk management plan
Answer: (SHOW ANSWER)
A comprehensive and documented IT risk management plan provides a structured approach to identifying, assessing, and mitigating IT risks. Integrating this plan into the organization's strategic planning ensures that IT risk considerations are aligned with business objectives and are factored into decision-making processes at the strategic level.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 1: Governance, Section: Risk Management Strategy.

NEW QUESTION: 25
Which of the following is the BEST metric to demonstrate the effectiveness of an organization's patch management process?
A. Average time to implement patches after vendor release
B. Number of patches tested prior to deployment
C. Increase in the frequency of patches deployed into production
D. Percent of patches implemented within established timeframe
Answer: (SHOW ANSWER)
The percent of patches implemented within established timeframe is the best metric to demonstrate the effectiveness of an organization's patch management process, as it measures how well the organization meets its patching objectives and reduces its exposure to vulnerabilities. This metric reflects the timeliness, completeness, and quality of the patching process, and can be compared against the organization's patch management policy and standards. A high percent of patches implemented within established timeframe indicates that the organization has a mature and efficient patch management process that minimizes the risk of security breaches or operational disruptions due to unpatched systems.
References:
*ISACA, Risk and Information Systems Control Review Manual, 7th Edition, 2020, p. 2501
*ISACA, Practical Patch Management and Mitigation2
*NIST, Guide to Enterprise Patch Management Planning3

NEW QUESTION: 26
A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?
A. Enable data encryption in the test environment.
B. Prevent the use of production data in the test environment

C. De-identify data before being transferred to the test environment.
D. Enforce multi-factor authentication within the test environment.
Answer: (SHOW ANSWER)
The best recommendation to address the situation where personal information from the production environment is required for testing purposes in non-production environments is to de-identify data before being transferred to the test environment. De-identification is the process of removing or modifying any personally identifiable information (PII) or other sensitive data from the data sets, such as names, addresses, phone numbers, email addresses, etc., so that the data cannot be traced back to specific individuals. De-identification protects the privacy and confidentiality of the data, while still allowing for testing, analysis, or training purposes. Enabling data encryption, preventing the use of production data, and enforcing multi-factor authentication are also useful measures, but they do not eliminate the risk of data breaches or unauthorized access to PII. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.3.1, page 3-21.

NEW QUESTION: 27
A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?
A. Request a regulatory risk reporting methodology
B. Require critical success factors (CSFs) for IT risks.
C. Establish IT-specific compliance objectives
D. Communicate IT key risk indicators (KRIs) and triggers
Answer: C (LEAVE A REPLY)
The first thing that should be done by IT governance to support the development of a new risk management plan to specifically address legal and regulatory risk scenarios is to establish IT-specific compliance objectives. Compliance objectives are the goals or targets that the organization sets to ensure that its IT activities and processes comply with the relevant laws, regulations, standards, and contracts. Compliance objectives help to define the scope, criteria, and expectations for the IT compliance program, and to align the IT compliance activities with the organization's strategy, risk appetite, and performance measures. Compliance objectives also help to communicate and demonstrate the organization's commitment and accountability for IT compliance to the internal and external stakeholders, such as the board, management, regulators, auditors, and customers. The other options are not the first thing that should be done, although they may be useful or necessary steps or components of the IT compliance program. Requesting a regulatory risk reporting methodology, requiring critical success factors (CSFs) for IT risks, and communicating IT key risk indicators (KRIs) and triggers are all activities that can help to implement and monitor the IT compliance program, but they require the prior definition and agreement of the IT compliance objectives. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.4.1, page 2-37.

NEW QUESTION: 28
An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

A. Review the risk identification process.
B. Inform the risk scenario owners.
C. Create a risk awareness communication plan.
D. Update the risk register.
Answer: (SHOW ANSWER)
The best course of action when an audit reveals that there are changes in the environment that are not reflected in the risk profile is to review the risk identification process. This is because the risk identification process is the first step in the risk management process and it is responsible for identifying and assessing the potential risks that may affect the organization's objectives. If the risk identification process is not effective, it may result in incomplete, inaccurate, or outdated risk profiles that do not reflect the current environment and the associated risks. Therefore, reviewing the risk identification process will help to ensure that the risk profile is updated and aligned with the changes in the environment and the organization's strategy. References = Responding to Audit Findings

NEW QUESTION: 29
Which of the following activities is PRIMARILY the responsibility of senior management?
A. Bottom-up identification of emerging risks
B. Categorization of risk scenarios against a standard taxonomy
C. Prioritization of risk scenarios based on severity
D. Review of external loss data
Answer: C (LEAVE A REPLY)
The primary responsibility of senior management in risk management is to prioritize the risk scenarios based on severity. Risk scenarios are hypothetical events or situations that could affect the achievement of the objectives. Risk severity is a measure of the overall level of risk, based on the combination of the probability and impact of the risk scenario. Prioritizing the risk scenarios based on severity is the primary responsibility of senior management, because it helps to allocate the resources and actions to the most critical and urgent risks, and to align the risk management process with the organizational strategy and risk appetite. Senior management also has the authority and accountability to make the final decisions and approve the risk response plans for the prioritized risks. The other options are not the primary responsibility of senior management, although they may be involved or consulted in these activities. Bottom-up identification of emerging risks is a process of identifying and reporting the new or changing risks that may arise from the operational or tactical level of the organization. This is usually the responsibility of the risk owners or the risk practitioners, who have the knowledge and experience of the specific functions and processes. Categorization of risk scenarios against a standard taxonomy is a process of classifying and organizing the risk scenarios into predefined categories or groups, based on their nature, source, or impact. This is usually the responsibility of the risk analysts or the risk coordinators, who have the skills and tools to perform the risk analysis and assessment. Review of external loss data is a process of collecting and analyzing the data and information on the losses or incidents that occurred in other organizations or industries, due to similar or related risks. This is usually the responsibility of the risk researchers or the risk consultants, who have the access and expertise to obtain and interpret the external data and information. References = The Role of

Executive Management in ERM - Corporate Compliance Insights, Guidelines on Risk Management Practices - Board and Senior Management, Risk Manager Job Description [+2023 TEMPLATE] - Workable

NEW QUESTION: 30

To enable effective risk governance, it is MOST important for senior management to:

A. Ensure security policies and procedures are documented.

B. Ensure the IT governance framework is up to date.

C. Gain a clear understanding of business risk and related ownership.

D. Communicate the risk management strategy across the organization.

Answer: (SHOW ANSWER)

NEW QUESTION: 31

Which of the following BEST enables effective risk reporting to the board of directors?

A. Presenting case studies of breaches from other similar organizations

B. Mapping risk scenarios to findings identified by internal audit

C. Communicating in terms that correlate to corporate objectives and business value

D. Reporting key metrics that indicate the efficiency and effectiveness of risk governance

Answer: (SHOW ANSWER)

Effective risk reporting to the board of directors requires communication that aligns with the organization's strategic goals and business value. By correlating risk information to corporate objectives, the board can better understand the implications of risks on the organization's performance and make informed decisions. This approach ensures that risk discussions are relevant and meaningful at the executive level.

Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 3: Risk Response and Reporting, Section: Risk Communication and Reporting.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32

Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

A. Tokenized personal data only in test environments

B. Data loss prevention tools (DLP) installed in passive mode

C. Anonymized personal data in non-production environments

D. Multi-factor authentication for access to non-production environments

Answer: (SHOW ANSWER)

Anonymizing personal data in non-production environments means replacing the real data with fictitious but realistic data that does not allow identification of the individuals. This is a good way to mitigate the risk of sensitive personal data leakage from a software development environment, as it reduces the exposure of the data to unauthorized access or misuse. Tokenizing personal data only in test environments is not sufficient, as the data may still be exposed in other non-production environments, such as development or staging. Data loss prevention tools (DLP) installed in passive mode may detect and report data leakage incidents, but they do not prevent them from happening. Multi-factor authentication for access to non-production environments may enhance the security of the access, but it does not protect the data from being leaked by authorized users or compromised by other means. References = CRISC Review Manual (Digital Version), page 226; CRISC Review Questions, Answers & Explanations Database, question 195.

NEW QUESTION: 33
when developing IT risk scenarios associated with a new line of business, which of the following would be MOST helpful to review?
A. Resource allocation plan
B. Cost-benefit analysis
C. Organizational threats
D. Competitor analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following should be the PRIMARY basis for establishing a priority sequence when restoring business processes after a disruption?
A. Recovery Time Objective (RTO)
B. Mean Time to Recover (MTTR)
C. Mean Time Between Failures (MTBF)
D. Recovery Point Objective (RPO)
Answer: (SHOW ANSWER)
RTO defines the acceptable downtime for business processes. It helps determine the order in which services must be restored to minimize business impact.
Reference:CRISC Manual - Domain 3: Risk Response, Slide 226-224

NEW QUESTION: 35
A risk practitioner's BEST guidance to help an organization develop relevant risk scenarios is to ensure the scenarios are:
A. Aligned with risk management capabilities.
B. Based on industry trends.
C. Related to probable events.
D. Mapped to incident response plans.
Answer: (SHOW ANSWER)

Risk scenarios should reflect probable events to ensure relevance and practicality in risk assessments. This guidance supports the Risk Identification and Scenario Development process.

NEW QUESTION: 36
The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:
A. the third-party website manager
B. the business process owner
C. IT security
D. the compliance manager
Answer: (SHOW ANSWER)
The risk associated with data loss from a website which contains sensitive customer information is best owned by the business process owner, as they are ultimately responsible for the business objectives and outcomes that depend on the website. The business process owner should ensure that the website is adequately protected and that the customer data is handled in compliance with the relevant laws and regulations. The third-party website manager, IT security, and the compliance manager are all involved in managing the risk, but they are not the owners. The third-party website manager is responsible for the technical aspects of the website, such as hosting, maintenance, and performance. IT security is responsible for implementing and monitoring the security controls and policies for the website. The compliance manager is responsible for ensuring that the website meets the regulatory and contractual requirements. However, none of these roles have the authority or accountability to own the risk, as they are not directly affected by the business impact of the data loss. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 47.

NEW QUESTION: 37
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?
A. User acceptance testing (UAT)
B. Database activity monitoring
C. Source code review
D. Vulnerability analysis
Answer: (SHOW ANSWER)
A source code review is the process of examining and analyzing the source code of an application to identify any vulnerabilities, errors, or flaws that may compromise the security, functionality, or performance of the application. A source code review is the most effective way to identify an application backdoor prior to implementation, as it can detect any hidden or unauthorized code that may allow unauthorized access, bypass security controls, or execute malicious commands. A source code review can also help to improve the quality and reliability of the application, and ensure compliance with the coding standards and best practices. References = CRISC Review Manual, 7th Edition, page 181.

NEW QUESTION: 38

An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap

B. Highlight news articles about data breaches

C. Evaluate the risk as a measure of probable loss

D. Verify if competitors comply with a similar policy

Answer: (SHOW ANSWER)

A risk is the possibility of an event that may have a negative impact on the achievement of an organization's objectives. A risk can be measured by the probability and impact of the event, which indicate the likelihood and consequence of the event. A risk manager is a person who is responsible for performing risk management activities, such as identifying, analyzing, evaluating, treating, monitoring, and communicating risks. When an organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention, the risk manager's best response to the business owner who challenges whether the situation is worth remediating is to evaluate the risk as a measure of probable loss, which means to estimate the potential harm or damage that may result from the non-compliance with the policy. By evaluating the risk as a measure of probable loss, the risk manager can provide the business owner with the rationale and justification for the risk remediation, and help the business owner to understand the cost-benefit analysis of the risk response. References = CRISC Review Manual, 7th Edition, page 63.

NEW QUESTION: 39

Who should be accountable for authorizing information system access to internal users?

A. Information security officer

B. Information security manager

C. Information custodian

D. Information owner

Answer: (SHOW ANSWER)

According to the ISACA Risk and Information Systems Control study guide and handbook, the information owner is the official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner is also responsible for authorizing access to the information within their domain, based on the principle of least privilege and the need to know. Therefore, the information owner should be accountable for authorizing information system access to internal users12

1: ISACA Risk and Information Systems Control Study Guide, 4th Edition, page 33 2: ISACA Risk and Information Systems Control Handbook, 1st Edition, page 25

NEW QUESTION: 40

Which of the following is the MOST significant benefit of using quantitative risk analysis instead of qualitative risk analysis?

Freecram.net

A. Minimized time to completion

B. Decreased structure

C. Minimized subjectivity

D. Decreased cost

Answer: (SHOW ANSWER)

Quantitative risk analysis provides numerical values for likelihood and impact, thereby reducing subjectivity. It enables risk practitioners to perform cost-benefit analysis and make data-driven decisions. Though time-consuming, its objectivity is its major advantage over qualitative methods.

Reference:CRISC Manual - Domain 2, Slide 186-187

NEW QUESTION: 41

Which of the following is a detective control?

A. Limit check

B. Periodic access review

C. Access control software

D. Rerun procedures

Answer: (SHOW ANSWER)

A detective control is a type of internal control that seeks to uncover problems in a company's processes once they have occurred. Examples of detective controls include physical inventory checks, reviews of account reports and reconciliations, as well as assessments of current controls1. A periodic access review is a detective control that involves verifying the access rightsand privileges of users to ensure that they are appropriate and authorized. A periodic access review can help to detect any unauthorized or inappropriate access, such as excessive or redundant permissions, segregation of duties violations, or dormant ororphaned accounts23. The other options are not detective controls, but rather preventive controls, which are designed to prevent errors or fraud from occurring in the first place. A limit check is a preventive control that validates the input data against a predefined range or limit, and rejects any data that falls outside the acceptable range4. Access control software is a preventive control that restricts the access to information systems or resources based on the identity, role, or credentials of the user5. Rerun procedures are preventive controls that ensure the accuracy and completeness of data processing by repeating the same process and comparing the results6. References = Detective Control: Definition, Examples, Vs. Preventive Control; Detective Control - What Is It, Examples, Vs Preventive Control; Limit Check - an overview | ScienceDirect Topics; Access Control Software - an overview | ScienceDirect Topics; Rerun Procedures - an overview | ScienceDirect Topics

NEW QUESTION: 42

Which of the following activities is a responsibility of the second line of defense?

A. Challenging risk decision making

B. Developing controls to manage risk scenarios

C. Implementing risk response plans

D. Establishing organizational risk appetite

Answer: (SHOW ANSWER)

The second line of defense is responsible for challenging the risk decision making of the first line of defense, which is the business process owners and managers. The second line of defense also provides oversight,

guidance, and support to the first line of defense in implementing and maintaining effective risk management practices. The second line of defense includes functions such as risk management, compliance, quality assurance, and internal audit. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.2: IT Risk Management Roles and Responsibilities, Page 14.

NEW QUESTION: 43
A cloud service provider has completed upgrades to its cloud infrastructure to enhance service availability. Which of the following is the MOST important key risk indicator (KRI) for management to monitor?
A. Peak demand on the cloud service during business hours
B. Percentage of technology upgrades resulting in security breaches
C. Number of incidents with downtime exceeding contract threshold
D. Percentage of servers not patched per policy
Answer: (SHOW ANSWER)
Monitoring the number of incidents with downtime exceeding the contract threshold is a critical KRI for assessing the effectiveness of infrastructure upgrades aimed at enhancing service availability. This metric directly reflects the provider's ability to meet agreed-upon service levels and helps identify areas requiring further improvement.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Key Risk Indicators.

NEW QUESTION: 44
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?
A. Trends in IT resource usage
B. Trends in IT maintenance costs
C. Increased resource availability
D. Increased number of incidents
Answer: A (LEAVE A REPLY)
IT capacity is the ability of an IT system or network to handle the current and future workload and performance demands. IT capacity can be affected by various factors, such as the number and type of users, applications, devices, data, transactions, etc. IT capacity management is the process of planning, monitoring, and optimizing the IT resources to ensure that they meet the business needs and objectives. IT capacity management can help prevent issues such as system slowdowns, outages, errors, or failures, and improve the efficiency, reliability, and security of the IT system or network. One of the IT key risk indicators (KRIs) that provides management with the best feedback on IT capacity is the trends in IT resource usage. IT resource usage is the measure of how much of the IT resources, such as CPU, memory, disk, bandwidth, etc., are being consumed by the IT system or network. Trends in IT resource usage can help monitor and analyze the changes in the IT capacity over time, and identify the patterns, peaks, and bottlenecks in the IT resource consumption. Trends in IT resource usage can also help forecast the future IT capacity requirements, and plan for the appropriate IT resource allocation, optimization, or expansion. Trends in IT resource usage can provide management with valuable information on the current and potential IT capacity risks, and support the

decision making and risk response for IT capacity management. References = Integrating KRIs and KPIs for Effective Technology Risk Management, p. 3-4.

NEW QUESTION: 45
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?
A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
B. The KRI is not providing useful information and should be removed from the KRI inventory.
C. The KRI threshold needs to be revised to better align with the organization s risk appetite
D. Senior management does not understand the KRI and should undergo risk training.
Answer: C (LEAVE A REPLY)
A key risk indicator (KRI) is a metric that measures the level and trend of a risk that may affect the organization's objectives, operations, or performance1. A KRI threshold is a predefined value or range that indicates the acceptable or tolerable level of risk for the organization2. The organization's risk appetite is the amount and type of risk that it is willing to take in order to meet its strategic goals3. Therefore, the most likely reason for senior management's response is that the KRI threshold needs to be revised to better align with the organization's risk appetite. This means that the current threshold is either too low or too high, resulting in false alarms or missed signals. By adjusting the threshold to reflect the organization's risk appetite, senior management can ensure that the KRI provides relevant and actionable information for risk management and decision making. The other options are not the most likely reasons for senior management's response, as they imply that the KRI is faulty, irrelevant, or misunderstood. The underlying data source for the KRI is using inaccurate data and needs to be corrected. This option assumes that the KRI is based on erroneous or unreliable data, which would affect its validity and reliability. However, this is not the most likely reason, as senior management would be expected to verify the data quality and accuracy before using the KRI for risk monitoring and reporting. The KRI is not providing useful information and should be removed from the KRI inventory. This option assumes that the KRI is not aligned with the organization's objectives, strategies, or risk profile, which would affect its usefulness and value. However, this is not the most likely reason, as senior management would be expected to review and update the KRI inventory periodically to ensure that the KRIs are relevant and meaningful for risk management. Senior management does not understand the KRI and should undergo risk training. This option assumes that senior management lacks the knowledge or skills to interpret and use the KRI for risk management, which would affect their competence and confidence. However, this is not the most likely reason, as senior management would be expected to have sufficient risk awareness and education to understand and apply the KRI for risk management. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.4, Page 53.

NEW QUESTION: 46
Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?
A. A comparison of the costs of notice and consent control options
B. Examples of regulatory fines incurred by industry peers for noncompliance

C. A report of critical controls showing the importance of notice and consent
D. A cost-benefit analysis of the control versus probable legal action
Answer: (SHOW ANSWER)
A cost-benefit analysis of the control versus probable legal action is the best way to inform decision-makers about the value of a notice and consent control for the collection of personal information, as it quantifies the potential benefits and costs of implementing the control and compares them with the potential consequences of not implementing the control. This helps the decision-makers to evaluate the trade-offs and the return on investment of the control.
A comparison of the costs of notice and consent control options is not sufficient to inform decision-makers about the value of the control, as it does not consider the benefits or the risks of the control.
Examples of regulatory fines incurred by industry peers for noncompliance are not the best way to inform decision-makers about the value of the control, as they are based on historical data and may not reflect the current or future situation of the enterprise.
A report of critical controls showing the importance of notice and consent is not the best way to inform decision-makers about the value of the control, as it does not provide any quantitative or comparative data to support the decision. References = CRISC Review Manual, 7th Edition, ISACA, 2020, page 140-1411

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the actin to address the risk associated with data transfer if the relationship is terminated with the vendor?
A. Meet with the business leaders to ensure the classification of their transferred data is in place
B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
D. Work closely with the information security officer to ensure the company has the proper security controls in place.
Answer: B (LEAVE A REPLY)
The best course of action to address the risk associated with data transfer if the relationship is terminated with the vendor is to ensure the language in the contract explicitly states who is accountable for each step of the data transfer process. This can help to avoid ambiguity, confusion, or disputes over the ownership, responsibility, and liability of the data and the data transfer process. Meeting with the business leaders,

collecting requirements, and working with the information security officer are important activities, but they are not as effective as ensuring the contractual agreement is clear and enforceable. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 4; CRISC Review Manual, 6th Edition, page 153.

NEW QUESTION: 48
A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:
A. mitigated
B. accepted
C. avoided
D. deferred
Answer: (SHOW ANSWER)
The risk practitioner should report that the associated risk has been deferred, as this means that the risk response has been postponed or delayed due to lack of resources or other constraints. Deferring a risk response implies that the risk owner acknowledges the risk and intends to implement the risk mitigation action plan at a later stage, when the resources or conditions are available. The other options are not correct, as they do not reflect the actual status of the risk response. Mitigating a risk means that the risk response has been implemented and the risk level has been reduced. Accepting a risk means that the risk response has been rejected or waived, and the risk level has been accepted as it is. Avoiding a risk means that the risk response has been implemented and the risk level has been eliminated or transferred. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk Response, page 146.

NEW QUESTION: 49
Which of the following would provide the BEST evidence of an effective internal control environment/?
A. Risk assessment results
B. Adherence to governing policies
C. Regular stakeholder briefings
D. Independent audit results
Answer: (SHOW ANSWER)
The best evidence of an effective internal control environment is the independent audit results. Independent audit results are the outcomes or findings of an external or independent party that evaluates the design, implementation, and operation of the internal controls. Independent audit results can provide an objective, reliable, and consistent assessment of the internal control environment, and identify the strengths, weaknesses, gaps, or issues of the internal controls. Independent audit results can also provide assurance, recommendations, or improvement opportunities for the internal control environment. The other options are not as good as independent audit results, as they are related to the inputs, processes, or outputs of the internal control environment, not the evaluation or verification of the internal control environment. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.3: IT Control Assessment, page 69.

NEW QUESTION: 50

Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

Freecram.net

A. Obsolete response documentation

B. Increased stakeholder turnover

C. Failure to audit third-party providers

D. Undefined assignment of responsibility

Answer: (SHOW ANSWER)

The most significant risk to an organization when updating the incident response plan is the undefined assignment of responsibility. An incident response plan is a document that defines the roles, responsibilities, procedures, and resources for responding to an incident that could disrupt the normal operations of the organization, or compromise its assets, reputation, or compliance. An incident response plan should clearly assign the responsibility for each task and activity involved in the incident response process, such as detection, containment, analysis, eradication, recovery, and reporting. Undefined assignment of responsibility could lead to confusion, duplication, conflict, or omission among the stakeholders, and impair the effectiveness and efficiency of the incident response process. Undefined assignment of responsibility could also increase the risk of escalation, recurrence, or impact of the incident, and affect the accountability and performance of the organization. Obsolete response documentation, increased stakeholder turnover, and failure to audit third-party providers are also risks, but they are not as significant as undefined assignment of responsibility, as they do not directly affect the execution and outcome of the incident response process. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 130.

NEW QUESTION: 51

Which of the following controls would BEST reduce the risk of account compromise?

A. Enforce password changes.

B. Enforce multi-factor authentication (MFA).

C. Enforce role-based authentication.

D. Enforce password encryption.

Answer: (SHOW ANSWER)

Multi-factor authentication (MFA)significantly reduces the risk of account compromise by requiring multiple forms of verification, such as a password and a one-time code, enhancing security beyond single-factor authentication methods.

NEW QUESTION: 52

An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

A. Invoke the disaster recovery plan during an incident.

B. Prepare a cost-benefit analysis of alternatives available

C. Implement redundant infrastructure for the application.

D. Reduce the recovery time by strengthening the response team.

Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), the next course of action when there is a gap between the acceptable downtime and the actual recovery time of an application is to prepare a cost-benefit analysis of alternatives available to reduce the gap. The cost-benefit analysis should compare the costs of implementing different risk response options, such as avoidance, mitigation, transfer or acceptance, with the benefits of reducing the impact and likelihood of the risk. The cost-benefit analysis should also consider the alignment of the risk response options with the enterprise's risk appetite, business objectives and strategy. The cost-benefit analysis should help the application owner and the risk owner to select the most appropriate risk response option that optimizes the value of the application and minimizes the residual risk.
References = CRISC Review Manual (Digital Version), Chapter 3: IT Risk Response, Section 3.2: Risk Response Process, pp. 162-1631

NEW QUESTION: 53
Senior leadership has set guidelines for the integration of a new acquisition. The guidelines allow for a variation in the level of risk-taking. The variation indicates which of the following risk management concepts?
A. Risk tolerance
B. Risk appetite
C. Risk sensitivity
D. Risk velocity
Answer: (SHOW ANSWER)
Risk tolerance refers to the acceptable level of variation in outcomes related to specific risks that an organization is willing to withstand. It defines the boundaries within which the organization can operate safely and is often set by senior leadership to guide decision-making processes. In the context of integrating a new acquisition, allowing for variation in the level of risk-taking directly pertains to the organization's risk tolerance.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 1: Governance, Section: Risk Governance.

NEW QUESTION: 54
Which of the following is the FIRST step in risk assessment?
A. Review risk governance
B. Asset identification
C. Identify risk factors
D. Inherent risk identification
Answer: B (LEAVE A REPLY)
The first step in risk assessment is asset identification, which is the process of identifying and documenting the assets that are relevant and valuable to the organization, such as people, information, systems, processes, or infrastructure1. Asset identification can help to:
* Establish the scope and boundaries of the risk assessment, and ensure that all the assets within the scope are considered and covered2.
* Determine the criticality and priority of the assets, and assign them appropriate values or ratings based on their importance and contribution to the organization's objectives3.

* Identify the potential threats and vulnerabilities that may affect the assets, and assess their likelihood and impact on the assets4.
The other options are not the first step in risk assessment, because:
* Review risk governance is not the first step, but rather a prerequisite or a foundation for risk assessment. Risk governance is the system of principles, policies, roles, and responsibilities that guide and oversee the risk management activities and initiatives of the organization5. Reviewing risk governance can help to ensure that the risk assessment is aligned with the organization's risk strategy, culture, and appetite, and that the risk assessment process is consistent, effective, and efficient6.
* Identify risk factors is not the first step, but rather a subsequent or a parallel step to asset identification. Risk factors are the elements or conditions that influence or contribute to the occurrence or outcome of a risk event7. Identifying risk factors can help to understand the causes and sources of the risks, and to analyze and evaluate the risks based on their probability and severity.
* Inherent risk identification is not the first step, but rather a later or a dependent step on asset identification and risk factor identification. Inherent risk is the level of risk that exists before the implementation of risk responses. Identifying inherent risk can help to measure the exposure or uncertainty of the assets, and to determine the need and extent of the risk responses.
References =
* Risk Governance - CIO Wiki
* Risk Governance Framework - CIO Wiki
* Asset Identification - CIO Wiki
* Asset Identification and Valuation - ISACA
* Asset Criticality - CIO Wiki
* Threat and Vulnerability Assessment - CIO Wiki
* Risk Factor - CIO Wiki
* [Risk Factor Analysis - CIO Wiki]
* [Inherent Risk - CIO Wiki]
* [Inherent Risk Assessment - CIO Wiki]
* [Risk Assessment - CIO Wiki]

NEW QUESTION: 55
Risk mitigation procedures should include:
A. buying an insurance policy.
B. acceptance of exposures
C. deployment of counter measures.
D. enterprise architecture implementation.
Answer: (SHOW ANSWER)
Risk mitigation procedures are the actions and plans that an organization implements to reduce the likelihood and impact of identified risks. Risk mitigation procedures should include the deployment of counter measures, which are the specific controls or solutions that address the root causes or sources of the risks, and prevent or minimize the potential losses or damages. For example, a counter measure for the risk of data breach could be encrypting the data or implementing a firewall. The deployment of counter measures

should be based on a cost-benefit analysis, a risk assessment, and a risk response strategy. The other options are not necessarily part of risk mitigation procedures. Buying an insurance policy is an example of risk transfer, which is a risk response strategy that shifts the responsibility or burden of the risk to another party, such as an insurer or a vendor. However, risk transfer does not eliminate or reduce the risk itself, and it may involve additional costs or conditions. Acceptance of exposures is an example of risk acceptance, which is a risk response strategy that acknowledges the existence and consequences of the risk, and decides not to take any action to change the risk situation. However, risk acceptance does not mitigate the risk, and it may require contingency plans or reserves to deal with the potential outcomes. Enterprise architecture implementation is an example of a business process or project that may involve or create risks, but it is not a risk mitigation procedure itself.
Enterprise architecture is the design and structure of an organization's IT systems, networks, and resources, and how they align with the organization's goals and strategies. Enterprise architecture implementation may require risk management activities, such as risk identification, assessment, and response, but it is not a risk mitigation procedure itself. References = Risk IT Framework, ISACA, 2022, p. 151

NEW QUESTION: 56
Which of the following is the MOST important consideration for protecting data assets m a Business application system?
A. Application controls are aligned with data classification lutes
B. Application users are periodically trained on proper data handling practices
C. Encrypted communication is established between applications and data servers
D. Offsite encrypted backups are automatically created by the application
Answer: (SHOW ANSWER)
The most important consideration for protecting data assets in a business application system is to ensure that the application controls are aligned with the data classification rules. Data classification rules define the level of sensitivity, confidentiality, and criticality of the data, and the corresponding security requirements and controls. Application controls are the policies, procedures, and technical measures that are implemented at the application level to ensure the security, integrity, and availability of the data. Application controls should be designed and configured to match the data classification rules, so that the data is protected according to its value and risk. For example, if the data is classified as highly confidential, the application controls should enforce strong authentication, encryption, access control, logging, and auditing mechanisms. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 214.

NEW QUESTION: 57
Zero Trust architecture is designed and deployed with adherence to which of the following basic tenets?
A. Incoming traffic must be inspected before connection is established.
B. Security frameworks and libraries should be leveraged.
C. Digital identities should be implemented.
D. All communication is secured regardless of network location.
Answer: (SHOW ANSWER)
Zero Trust Architecture:

* Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside their perimeters and must verify everything attempting to connect to their systems.
Basic Tenets of Zero Trust:
* The primary principle is "never trust, always verify." This means every access request is authenticated, authorized, and encrypted regardless of where it originates.
* Zero Trust requires securing all communication, whether it occurs within the internal network or comes from external sources. This approach prevents lateral movement by potential attackers who have breached the network perimeter.
Key Components:
* Authentication and Authorization: Continuous verification of user identities and access privileges.
* Microsegmentation: Dividing the network into small, isolated segments to limit the spread of threats.
* Encryption: Ensuring that all data, whether at rest or in transit, is encrypted to protect its confidentiality and integrity.
Other Options:
* Incoming Traffic Inspection: While important, this is just one aspect of Zero Trust.
* Security Frameworks and Libraries: These are tools and guidelines to implement security but do not define the core tenets of Zero Trust.
* Digital Identities: Implementing digital identities is part of the broader Zero Trust strategy but not a standalone tenet.
References:
* The CISSP Study Guide explains the Zero Trust architecture and its emphasis on securing all communications regardless of network location (Sybex CISSP Study Guide, Chapter 8: Principles of Security Models, Design, and Capabilities).

NEW QUESTION: 58
An organization's risk profile indicates that residual risk levels have fallen significantly below management's risk appetite. Which of the following is the BEST course of action?
A. Add more risk scenarios to the risk register.
B. Increase risk appetite.
C. Decrease monitoring of residual risk levels.
D. Optimize controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
A risk practitioner observes that hardware failure incidents have been increasing over the last few months. However, due to built-in redundancy and fault-tolerant architecture, there have been no interruptions to business operations. The risk practitioner should conclude that:
A. a root cause analysis is required
B. controls are effective for ensuring continuity
C. hardware needs to be upgraded
D. no action is required as there was no impact

Answer: (SHOW ANSWER)

According to the Risk and Information Systems Control documents, the risk practitioner should conclude that no action is required as there was no impact. The fact that there have been no interruptions to business operations despite the increasing hardware failure incidents indicates that the built-in redundancy and fault-tolerant architecture are effective in ensuring continuity.

Options A and C are not necessary in this scenario. A root cause analysis (Option A) might be considered if there were actual interruptions or impact on business operations. However, since there were no interruptions, a root cause analysis may not be immediately required. Similarly, upgrading hardware (Option C) may not be necessary if the existing controls are effectively preventing business disruptions.

References = Risk and Information Systems Control Study Manual

NEW QUESTION: 60

Which of the following BEST helps to balance the costs and benefits of managing IT risk?

A. Prioritizing risk responses

B. Evaluating risk based on frequency and probability

C. Considering risk factors that can be quantified

D. Managing the risk by using controls

Answer: (SHOW ANSWER)

Prioritizing risk responses helps to balance the costs and benefits of managing IT risk by ensuring that the most significant risks are addressed first and that the resources allocated to risk management are used efficiently and effectively. Evaluating risk based on frequency and probability is a part of risk analysis, not risk response. Considering risk factors that can be quantified is also a part of risk analysis, and it does not necessarily capture all the relevant aspects of risk. Managing the risk by using controls is a possible risk response, but it does not guarantee that the costs and benefits of risk management are balanced, as some controls may be too expensive or ineffective for the level of risk they mitigate. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk Response, page 145.

NEW QUESTION: 61

During a risk assessment, what should an assessor do after identifying threats to organizational assets?

A. Request funding for the security program

B. Determine threats to be reported to upper management

C. Implement controls to achieve target risk levels

D. Evaluate the controls currently in place

Answer: (SHOW ANSWER)

The CRISC risk assessment process follows a sequence:

* Identify assets #
* Identify threats #
* Identify vulnerabilities #
* Evaluate existing controls #
* Assess likelihood and impact.

Per ISACA CRISC guidance:

"After identifying threats, the next step is to evaluate the effectiveness of existing controls to determine residual risk." Implementing new controls (Option C) happens after risk evaluation and treatment planning. Hence, D. Evaluate the controls currently in place is correct.
CRISC Reference: Domain 2 - IT Risk Assessment, Topic: Risk Identification and Control Evaluation Steps.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
Which of the following BEST enables the identification of trends in risk levels?
A. Correlation between risk levels and key risk indicators (KRIs) is positive.
B. Measurements for key risk indicators (KRIs) are repeatable
C. Quantitative measurements are used for key risk indicators (KRIs).
D. Qualitative definitions for key risk indicators (KRIs) are used.
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics or measures that provide information on the current or potential exposure and performance of an organization in relation to specific risks. KRIs can help to monitor and track the changes or trends in the risk level and the risk response over time, identify and alert the risk issues or events that require attention or action, evaluate and report the effectiveness and efficiency of the risk management processes and practices, and support and inform the risk decision making and improvement1. The best way to enable the identification of trends in risk levels is to ensure that the correlation between risk levels and KRIs is positive, because it means that the KRIs are aligned with and reflective of the risk levels, and that they can capture and indicate the variations or movements in the risk levels accurately and reliably. A positive correlation between risk levels and KRIs can be achieved by:
Selecting and defining the KRIs that are relevant and appropriate for the specific risks that the organization faces, and that are consistent and comparable across different domains and contexts Collecting and analyzing the data and information that are reliable and sufficient for the KRIs, and that are sourced from various methods and sources, such as risk assessments, audits, monitoring, alerts, or incidents Applying and using the tools and techniques that are suitable and feasible for the KRIs, such as risk matrices, risk registers, risk indicators, or risk models Reviewing and updating the KRIs periodically or as needed, and ensuring that they reflect the current or accurate risk levels, which may change over time or due to external factors23 The other options are not the best ways to enable the identification of trends in risk levels, but rather some of the factors or aspects of KRIs. Measurements for KRIs are repeatable is a factor that can enhance the reliability and validity of the KRIs, as it means that the KRIs can produce the same or similar results under the same or similar conditions. However, repeatability does not necessarily imply accuracy or sensitivity, and it may not capture or reflect the changes or trends in the risk levels. Quantitative

measurements are used for KRIs is an aspect that can improve the objectivity and precision of the KRIs, as it means that the KRIs are expressed in numerical or measurable values, such as percentages, probabilities, or monetary amounts.
However, quantitative measurements may not be suitable or feasible for all types of risks or KRIs, and they may not capture or reflect the complexity or uncertainty of the risk levels. Qualitative definitions for KRIs are used is an aspect that can enhance the understanding and communication of the KRIs, as it means that the KRIs are expressed in descriptive or subjective terms, such as high, medium, or low, based on criteria such as likelihood, impact, or severity. However, qualitative definitions may not be consistent or comparable across different risks or KRIs, and they may not capture or reflect the magnitude or variation of the risk levels. References = Key Risk Indicators: What They Are and How to Use Them Key Risk Indicators: A Practical Guide | SafetyCulture Key Risk Indicators: Types and Examples
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 63
When an organization's disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?
A. Acceptance
B. Mitigation
C. Transfer
D. Avoidance
Answer: (SHOW ANSWER)
A reciprocal agreement is an agreement made by two or more organizations to use each other's resources during a disaster1. For example, two organizations with similar IT infrastructure may agree to provide backup servers or data centers for each other in case of a major disruption. By doing so, they transfer the risk of losing their IT capabilities to the other party, who agrees to share the responsibility and cost of recovery.
A reciprocal agreement is a form of risk transfer, which is one of the four risk treatment options according to ISO 270012. Risk transfer means that the organization shifts the potential negative consequences of a risk to another party, such as an insurance company, a vendor, or a partner. This reduces the organization's exposure and liability to the risk, but it does not eliminate the risk completely, as the other party may fail to fulfill their obligations or charge a high price for their services.
References = Reciprocal Agreement - Risky Thinking, ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide - Advisera

NEW QUESTION: 64
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:
A. the proposed controls are implemented as scheduled.
B. security controls are tested prior to implementation.
C. compliance with corporate policies.
D. the risk response strategy has been decided.
Answer: (SHOW ANSWER)

The primary reason for tracking the status of risk mitigation plans is to ensure that the proposed controls are implemented as scheduled, as this can help to reduce the risk exposure of the organization and to achieve the desired risk objectives. Tracking the status of risk mitigation plans can also help to monitor and evaluate the performance and effectiveness of the risk controls, and to identify and address any issues or gaps that may arise during the implementation. Tracking the status of risk mitigation plans can also provide feedback and information to the risk owners and stakeholders, and enable them to adjust the risk strategy and response actions accordingly. References = CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 251. CRISC Sample Questions 2024, Question 251. ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 251. CRISC by Isaca Actual Free Exam Q&As, Question 9.

NEW QUESTION: 65
Which of the following is the PRIMARY reason to ensure policies and standards are properly documented within the risk management process?
A. It facilitates the use of a framework for risk management.
B. It establishes a means for senior management to formally approve risk practices.
C. It encourages risk-based decision making for stakeholders.
D. It provides a basis for benchmarking against industry standards.
Answer: (SHOW ANSWER)
Policies and standards are important components of the risk management process, as they define the objectives, expectations, and requirements for managing risk within the organization. Policies and standards are also the means by which senior management formally approves and communicates the risk practices to the stakeholders, ensuring that the risk management process is aligned with the organizational strategy, culture, and values. Policies and standards also provide the authority and accountability for the risk management roles and responsibilities, as well as the criteria and metrics for measuring and reporting risk performance.

NEW QUESTION: 66
Which of the following MUST be updated to maintain an IT risk register?
A. Expected frequency and potential impact
B. Risk tolerance
C. Enterprise-wide IT risk assessment
D. Risk appetite
Answer: (SHOW ANSWER)
An IT risk register is a document that records and tracks the significant IT risks that an organization faces across its various functions, processes, and activities. An IT risk register can help to provide a comprehensive and consistent view of the organization's IT risk profile, and to support the decision making and reporting of the IT risk management function1.
One of the data that must be updated to maintain an IT risk register is the expected frequency and potential impact of each IT risk. The expected frequency is the probability or likelihood of the IT risk occurring, based on historical data, statistical analysis, expert judgment, or other methods. The potential impact is the

magnitude or severity of the consequences or outcomes of the IT risk, measured in terms of cost, time, quality, reputation, or other criteria2.
Updating the expected frequency and potential impact of each IT risk is essential for maintaining an IT risk register, because it can help to:
Evaluate and prioritize the IT risks based on their risk level, which is calculated by multiplying the frequency and impact Monitor and track the changes or trends in the IT risk exposure and performance over time Identify and implement the appropriate risk response strategies and controls, based on the risk level and the risk appetite and tolerance of the organization Report and communicate the IT risk status and progress to the stakeholders, using risk indicators, dashboards, or matrices3 The other options are not the data that must be updated to maintain an IT risk register, but rather the data that are used as inputs or outputs of the IT risk management process. Risk tolerance is the acceptable variation in the outcomes related to specific objectives or risks. Risk tolerance is used to measure the IT risk analysis and to guide the IT risk response. Enterprise-wide IT risk assessment is a process that identifies, analyzes, and evaluates the IT risks across theorganization. Enterprise-wide IT risk assessment is used topopulate the IT risk register and to inform the IT risk response. Risk appetite is the amount and type of risk that an organization is willing to accept in order to achieve its objectives. Risk appetite is used to guide the IT risk analysis and to align the IT risk response.
References = Risk Register - ISACA Risk Analysis - ISACA Risk Register 2021-2022 - UNECE
[How To Conduct Business Impact Analysis in 8 Easy Steps - G2]
[Risk Appetite and Risk Tolerance - ISACA]
[Enterprise Risk Assessment - ISACA]
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 67
Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?
A. Audit and compliance management
B. The chief information officer (CIO) and the chief financial officer (CFO)
C. Enterprise risk management and business process owners
D. Executive management and the board of directors
Answer: (SHOW ANSWER)
The stakeholders who are PRIMARILY responsible for determining enterprise IT risk appetite are the executive management and the board of directors, because they are the ones who set the strategic direction and objectives of the enterprise, and who define the acceptable level of risk exposure and tolerance for achieving those objectives. The other options are not the primary stakeholders, because:
* Option A: Audit and compliance management are responsible for providing assurance and oversight on the effectiveness of the risk management process and the compliance with internal and external requirements, but they do not determine the enterprise IT risk appetite.
* Option B: The CIO and the CFO are responsible for managing the IT resources and the financial resources of the enterprise, respectively, but they do not determine the enterprise IT risk appetite.
* Option C: Enterprise risk management and business process owners are responsible for identifying, assessing, and responding to the risks that affect their domains, but they do not determine the enterprise IT

risk appetite. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 83.

NEW QUESTION: 68
A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?
A. Risk forecasting
B. Risk tolerance
C. Risk likelihood
D. Risk appetite
Answer: (SHOW ANSWER)
Recovery time objectives (RTOs) are the maximum acceptable time frames for restoring the critical functions and processes after a disruption1. RTOs are derived from the business impact analysis (BIA) and reflect the organization's risk appetite, which is the amount of risk that an organization is willing to accept to achieve its objectives2. Risk tolerance is the level of risk a company is willing to tolerate, and it is affected by a number of factors, including how much uncertainty or financial loss can be tolerated and where those losses will impact operations3. Risk tolerance is used to measure if the risk exposure is within the risk appetite and to implement controls to reduce the residual risk to an acceptable level2. If the majority of core IT application RTOs have exceeded the maximum time defined by the business application owners, it means that the organization is not meeting its risk appetite and is exposed to more risk than it can accept. Therefore, the most likely change as a result is to adjust the risk tolerance to reflect the current reality and to take actions to improve the recovery capabilities and reduce the risk exposure4. Risk forecasting is the process of estimating the potential outcomes and impacts of future events that may affect the organization's objectives5. Risk forecasting may change as a result of the RTOs exceeding the maximum time, but it is not the most likely change, as it does not directly address the gap between the risk appetite and the risk exposure. Risk likelihood is the probability of a risk event occurring5. Risk likelihood may change as a result of the RTOs exceeding the maximum time, but it is not the most likely change, as it does not directly measure the impact of the risk event on the organization's objectives. Risk appetite is the amount of risk that an organization is willing to accept to achieve its objectives2. Risk appetite may change as a result of the RTOs exceeding the maximum time, but it is not the most likely change, as it is a strategic decision that reflects the organization's vision and mission, and not a tactical response to a specific risk event. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk Response and Mitigation, Section 5.3: Business Continuity Planning, pp. 227-238.

NEW QUESTION: 69
Which of the following is the PRIMARY purpose of creating and documenting control procedures?
A. To facilitate ongoing audit and control testing
B. To help manage risk to acceptable tolerance levels
C. To establish and maintain a control inventory
D. To increase the likelihood of effective control operation

Answer: (SHOW ANSWER)

The primary purpose of creating and documenting control procedures is to help manage risk to acceptable tolerance levels. Control procedures are the specific actions or steps that are performed to achieve the control objectives and mitigate the risks. Control procedures should be documented to provide clear guidance, consistency, and accountability for the control activities. Documenting control procedures also helps to monitor and evaluate the effectiveness and efficiency of the controls, and to identify and address any gaps or weaknesses. The other options are not the primary purpose of creating and documenting control procedures, although they may be secondary benefits or outcomes. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.2, page 1-15.

NEW QUESTION: 70

Which of the following is MOST helpful to facilitate the decision of recovery priorities in a disaster situation?

Freecram.net

A. Business Impact Analysis (BIA)

B. Key Risk Indicators (KRIs)

C. Recovery Point Objective (RPO)

D. Risk Scenario Analysis

Answer: (SHOW ANSWER)

A BIA identifies critical processes and interdependencies, enabling prioritization of recovery efforts based on business impact.

Reference:CRISC Manual - Domain 2 and 3, Slide 219-226

NEW QUESTION: 71

Which of the following BEST enables an organization to address new risk associated with an Internet of Things (IoT) solution?

A. Transferring the risk

B. Introducing control procedures early in the life cycle

C. Updating the risk tolerance to include the new risk

D. Implementing IoT device monitoring software

Answer: (SHOW ANSWER)

Introducing control procedures early in the IoT solution life cycle ensures proactive identification and mitigation of risks. This approach aligns withSecure System Development PracticesandRisk Mitigation Strategies, reducing exposure as the solution evolves.

NEW QUESTION: 72

Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

A. Increased time to remediate vulnerabilities

B. Inaccurate reporting of results

C. Increased number of vulnerabilities

D. Network performance degradation

Answer: (SHOW ANSWER)

The greatest concern for a risk practitioner with the use of a vulnerability scanning tool is the inaccurate reporting of results. A vulnerability scanning tool is a software that scans the network or system for known vulnerabilities and generates a report of the findings. However, the tool may produce false positives (reporting vulnerabilities that do not exist) or false negatives (missing vulnerabilities that do exist). This can lead to incorrect risk assessment, ineffective risk response, and wasted resources. Increased time to remediate vulnerabilities, increased number of vulnerabilities, and network performance degradation are other possible concerns, but they are not as critical as the inaccurate reporting of results. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 7; CRISC Review Manual, 6th Edition, page 202.

NEW QUESTION: 73

An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

A. Threat

B. Risk

C. Vulnerability

D. Policy violation

Answer: (SHOW ANSWER)

Documenting user IDs and passwords in procedure manuals is a vulnerability that exposes the organization to unauthorized access, data breaches, and other security risks. A vulnerability is a weakness or flaw in a system, process, or control that can be exploited by a threat. A threat is a potential cause of an unwanted incident that may harm the system or organization. A risk is the combination of the likelihood and impact of a threat exploiting a vulnerability. A policy violation is an act of non-compliance with a rule or standard that is established by the organization. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 8; CRISC Review Manual, 6th Edition, page 67.

NEW QUESTION: 74

Which of the following is the PRIMARY reason to use administrative controls in conjunction with technical controls?

A. To gain stakeholder support for the implementation of controls

B. To comply with industry best practices by balancing multiple types of controls

C. To improve the effectiveness of controls that mitigate risk

D. To address multiple risk scenarios mitigated by technical controls

Answer: (SHOW ANSWER)

Administrative controls, such as policies, procedures, and training, complement technical controls by addressing the human and organizational aspects of risk management. Using bothtypes of controls together enhances the overall effectiveness of the risk mitigation strategy, ensuring that technical measures are supported by appropriate governance and user behavior.

Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Control Types and Implementation.

NEW QUESTION: 75
The BEST way to improve a risk register is to ensure the register:
A. is updated based upon significant events.
B. documents possible countermeasures.
C. contains the risk assessment completion date.
D. is regularly audited.
Answer: (SHOW ANSWER)
A risk register is a tool that records and tracks the identified risks, their causes, impacts, probabilities, responses, and owners. It is a living document that should be updated regularly to reflect the changes in therisk environment and the status of the risk responses12. The best way to improve a risk register is to ensure that it is updated based upon significant events, such as:
New risks are identified or existing risks are eliminated
Risk probabilities or impacts change due to internal or external factors Risk responses are implemented or modified Risk owners or stakeholders change Risk incidents or issues occur Risk thresholds or appetite change Risk reporting or communication requirements change Updating the risk register based upon significant events can help to:
Maintain the accuracy and relevance of the risk information
Enhance the risk awareness and accountability of the risk owners and stakeholders Support the risk monitoring and reporting activities Facilitate the risk evaluation and decision-making processes Improve the risk management performance and maturity References = Risk Register - Project Management Knowledge How to Create a Risk Register: A Step-by-Step Guide - ProjectManager.com

NEW QUESTION: 76
Which of the following management actions will MOST likely change the likelihood rating of a risk scenario related to remote network access?
A. Creating metrics to track remote connections
B. Updating remote desktop software
C. Implementing multi-factor authentication (MFA)
D. Updating the organizational policy for remote access
Answer: (SHOW ANSWER)
Implementing multi-factor authentication (MFA) directly reduces the likelihood of unauthorized access by adding an extra layer of verification to remote network access. ISACA and CRISC materials emphasize that technical controls (e.g., MFA) meaningfully reduce the probability of threat scenarios involving remote access

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated**

and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
The software version of an enterprise's critical business application has reached end-of-life and is no longer supported by the vendor. IT has decided to develop an in-house replacement application. Which of the following should be the PRIMARY concern?
A. The system documentation is not available.
B. Enterprise risk management (ERM) has not approved the decision.
C. The board of directors has not approved the decision.
D. The business process owner is not an active participant.
Answer: (SHOW ANSWER)
The primary concern when IT decides to develop an in-house replacement application for a critical business application is that the business process owner is not an active participant. The business process owner is the person who has the authority and responsibility for the business process that is supported by the application, and who understands the business requirements, objectives, and expectations of the application. The business process owner should be involved in all stages of the application development lifecycle, from planning, analysis, design, testing, implementation, to maintenance, to ensure that the application meets the business needs and delivers value. Without the active participation of the business process owner, the application development project may face risks such as scope creep, miscommunication, user dissatisfaction, poor quality, or failure.
References:
*ISACA, Auditing IT Risk Associated With Change Management and Application Development1
*ISACA, Auditing Applications, Part 12

NEW QUESTION: 78
A risk practitioner has been made aware of a problem in an IT system that was missed during a routine risk assessment. Which of the following is the practitioner's BEST course of action?
A. Record the problem as a new issue in the risk management system
B. Record a new issue but backdate it to the original risk assessment date
C. Report the vulnerability to the asset owner's manager
D. Document the issue during the next risk assessment
Answer: A (LEAVE A REPLY)
Thebest practiceis torecord the problem immediately as a new issuein the risk management system. ISACA emphasizes maintaining an up-to-date risk register to ensure emerging issues are tracked and addressed in a timely manner.

NEW QUESTION: 79
Which of the following management actions will MOST likely change the likelihood rating of a risk scenario related to remote network access?

A. Creating metrics to track remote connections
B. Updating the organizational policy for remote access
C. Updating remote desktop software
D. Implementing multi-factor authentication
Answer: (SHOW ANSWER)
Automated asset management software is the best method to track asset inventory, as it can provide accurate, timely, and comprehensive information about the organization's IT assets, such as their location, status, configuration, ownership, and value. Automated asset management software can also help to optimize the utilization, performance, and lifecycle of the IT assets, and to reduce the risks of loss, theft, damage, or obsolescence. Automated asset management software can integrate with other systems, such as configuration management database (CMDB), service desk, and security tools, to enable better visibility, control, and governance of the IT assets.
References:
*ISACA, IT Asset Valuation, Risk Assessment and Control Implementation Model1
*ISACA, IT Asset Management: It's All About Process2
*ISACA, IT Asset Management Audit/Assurance Program3

NEW QUESTION: 80
The acceptance of control costs that exceed risk exposure is MOST likely an example of:
A. low risk tolerance.
B. corporate culture misalignment.
C. corporate culture alignment.
D. high risk tolerance
Answer: (SHOW ANSWER)
Corporate culture is the set of values, beliefs, and norms that shape the behavior and attitude of an organization and its people. Corporate culture alignment is the degree of consistency and compatibility between the corporate culture and the organization's vision, mission, strategy, and objectives. Corporate culture misalignment is the situation where the corporate culture is not aligned with the organization's goals and expectations, and may hinder or undermine the achievement of those goals. The acceptance of control costs that exceed risk exposure is most likely an example of corporate culture misalignment, as it indicates that the organization is not following a rational and optimal approach to risk management. The organization is spending more resources on controlling risks than the potential benefits or losses that the risks entail, which may result in inefficiency, waste, or opportunity cost. The organization may also be overemphasizing the importance of risk avoidance or mitigation, and neglecting the potential value creation or innovation that may arise from taking or accepting some risks. The other options are not the best answers, as they do not explain the situation of accepting control costs that exceed risk exposure. Low risk tolerance is the degree of variation from the risk appetite that the organization is not willing to accept. Low risk tolerance may lead to excessive or unnecessary controls, but it does not necessarily mean that the control costs exceed the risk exposure. High risk tolerance is the degree of variation from the risk appetite that the organization is willing to accept. High risk tolerance may lead to insufficient or ineffective controls, but it does not imply that the control costs exceed the risk exposure. Corporate culture alignment is the situation where the corporate

culture is aligned with the organization's goals and expectations, and supports and facilitates the achievement of those goals. Corporate culture alignment would not result in accepting control costs that exceed risk exposure, as it would imply a balanced and rational approach to risk management. References = CRISC Review Manual, pages 22-231; CRISC Review Questions, Answers & Explanations Manual, page 812

NEW QUESTION: 81
Which of the following is the PRIMARY accountability for a control owner?
A. Communicate risk to senior management.
B. Own the associated risk the control is mitigating.
C. Ensure the control operates effectively.
D. Identify and assess control weaknesses.
Answer: (SHOW ANSWER)
The primary accountability for a control owner is to ensure the control operates effectively, as they have the authority and responsibility to design, implement, monitor, and report on the performance and adequacy of the control, and to identify and address any control gaps or deficiencies. Communicating risk to senior management, owning the associated risk the control is mitigating, and identifying and assessing control weaknesses are not the primary accountabilities, as they are more related to the roles and responsibilities of the risk owner, the risk practitioner, or the auditor, respectively, rather than the control owner. References = CRISC Review Manual, 7th Edition, page 101.

NEW QUESTION: 82
An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:
A. chief risk officer.
B. project manager.
C. chief information officer.
D. business process owner.
Answer: (SHOW ANSWER)
The business process owner should be the risk owner for the risk exposure due to weak technical controls in a newly implemented HR system, because they are responsible for the performance and outcomes of the HR business process, and they understand the business requirements, expectations, and impact of the HR system.
The business process owner can also evaluate the trade-offs between the potential benefits and costs of the HR system, and the potential risks and consequences of a failure or breach of the system. The business process owner can also communicate and justify their risk acceptance or mitigation decision to the senior management and other stakeholders, and ensure that the risk is monitored and reviewed regularly. The other options are less appropriate to be the risk owner for this risk exposure. The chief risk officer is responsible for overseeing the enterprise-wide risk management framework and process, which includesensuring the identification, assessment, and reporting of risks. However, they are not the owner of the HR system or the HR business process, and they may not have the full knowledge or authority to accept or mitigate the risk on

behalf of the business. The project manager is responsible for managing the implementation of the HR system, which includes ensuring the delivery of the system within the scope, time, and budget constraints. However, they are not the owner of the HR system or the HR business process, and they may not have the full knowledge or authority to accept or mitigate the risk on behalf of the business. The chief information officeris responsible for managing the IT function and resources, which includes providing the technical support and security for the HR system. However, they are not the owner of the HRsystem or the HR business process, and they may not have the full knowledge or authority to accept or mitigate the risk on behalf of the business. References = Getting risk ownership right 1

NEW QUESTION: 83
During a risk assessment of a financial institution, a risk practitioner discovers that tellers can initiate and approve transactions of significant value. This team is also responsible for ensuring transactions are recorded and balances are reconciled by the end of the day. Which of the following is the risk practitioner's BEST recommendation to mitigate the associated risk?
A. Require a code of ethics.
B. Require a second level of approval.
C. Implement continuous monitoring.
D. Implement separation of duties.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?
A. KRIs assist in the preparation of the organization's risk profile.
B. KRIs signal that a change in the control environment has occurred.
C. KRIs provide a basis to set the risk appetite for an organization
D. KRIs provide an early warning that a risk threshold is about to be reached.
Answer: (SHOW ANSWER)
The main benefit of using key risk indicators (KRIs) for an organization is that they provide an early warning that a risk threshold is about to be reached. KRIs are metrics that measure the likelihood and impact of risks, and help monitor and prioritize the most critical risks. KRIs also help to trigger timely and appropriate risk responses, before the risk becomes unmanageable or unacceptable. The other options are not the main benefit of using KRIs, although they may be secondary benefits or outcomes. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.4.1, page 4-36.

NEW QUESTION: 85
When reviewing a business continuity plan (BCP). which of the following would be the MOST significant deficiency?
A. BCP testing is net in conjunction with the disaster recovery plan (DRP)
B. Recovery time objectives (RTOs) do not meet business requirements.
C. BCP is often tested using the walk-through method.
D. Each business location has separate, inconsistent BCPs.

Answer: (SHOW ANSWER)

According to the CRISC Review Manual, recovery time objectives (RTOs) are the maximum acceptable time that an IT system can be inoperable without causing significant damage to the business operations and objectives. RTOs are determined by the business impact analysis (BIA) and are used to define the recovery strategies and priorities. Therefore, if the RTOs do not meet the business requirements, it would be the most significant deficiency in the BCP, as it would imply that the recovery plan is not aligned with the business needs and expectations. The other options are not the most significant deficiencies, as they do not directly affect the recovery time and the business continuity. BCP testing is not necessarily done in conjunction with the DRP, as they have different scopes and objectives. BCP testing can use different methods, such as walk-through, simulation, or full interruption, depending on the purpose and scope of the test. Each business location can have separate BCPs, as long as they are consistent with the enterprise-wide BCP and the business requirements. References = CRISC Review Manual, 7th Edition, Chapter 5, Section 5.2.2, page 240.

NEW QUESTION: 86

Which of the following is MOST important when discussing risk within an organization?

A. Adopting a common risk taxonomy

B. Using key performance indicators (KPIs)

C. Creating a risk communication policy

D. Using key risk indicators (KRIs)

Answer: (SHOW ANSWER)

A common risk taxonomy is a framework that defines and categorizes the sources, types, and impacts of risks within an organization1. It helps to establish a consistent and shared understanding of risk across the organization, and to facilitate effective risk identification, assessment, reporting, and communication2. A common risk taxonomy also enables comparison and aggregation of risks at different levels and domains, and supports alignment of risk management with business objectives and strategies3. Using key performance indicators (KPIs) and key risk indicators (KRIs) are important for measuring and monitoring risk and performance, but they are not the most important factor when discussing risk within an organization. KPIs and KRIs should be derived from the common risk taxonomy and aligned with the organization's risk appetite and tolerance4. Creating a risk communication policy is also important for ensuring that risk information is communicated to the right stakeholders at the right time and in the right format, but it is not the most important factor either. A risk communication policy should be based on the common risk taxonomy and the risk roles and responsibilities within the organization5. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.2: Risk Taxonomy, pp. 25-29.

NEW QUESTION: 87

Which of the following cloud service models is MOST appropriate for client organizations that want to maximize their control over management of the data life cycle?

A. Data as a Service (DaaS)

B. Infrastructure as a Service (IaaS)

C. Platform as a Service (PaaS)

D. Software as a Service (SaaS)

Answer: (SHOW ANSWER)

Infrastructure as a Service (IaaS) provides organizations with the highest level of control over their IT resources in the cloud. With IaaS, clients manage the operating systems, storage, deployed applications, and possibly limited control of select networking components. This level of control allows organizations to manage the data life cycle comprehensively, including data creation, storage, processing, and disposal. In contrast, PaaS and SaaS models abstract more of these controls, limiting the client's ability to manage the data life cycle directly.

Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Cloud Computing Models.

NEW QUESTION: 88

Which of the following BEST mitigates the risk associated with inadvertent data leakage by users who work remotely?

A. Conducting training on the protection of organizational assets

B. Configuring devices to use virtual IP addresses

C. Ensuring patching for end-user devices

D. Providing encrypted access to organizational assets

Answer: (SHOW ANSWER)

Providing encrypted access to organizational assets is the best method to mitigate the risk of inadvertent data leakage by remote workers. Encryption ensures that data remains secure, even if accessed over unsecured networks.

NEW QUESTION: 89

During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

A. Implement compensating controls to reduce residual risk

B. Escalate the issue to senior management

C. Discuss risk mitigation options with the risk owner.

D. Certify the control after documenting the concern.

Answer: (SHOW ANSWER)

The best recommendation to the control owner when an existing control has deteriorated over time is to discuss risk mitigation options with the risk owner. This is because the risk owner is the person or entity who has the authority and accountability to make decisions and take actions regarding the risk, including the selection and implementation of the risk response strategies. The control owner is the person or entity who is responsible for the design, operation, and maintenance of the control, but not for the overall risk management.

By discussing risk mitigation options with the risk owner, the control owner can communicate the current status and performance of the control, and collaborate on finding the most appropriate and effective solution to address the risk and the control deterioration. The other options are not the best recommendation to the

control owner, because they do not involve the risk owner, who is the key stakeholder in the risk management process, as explained below:
A). Implement compensating controls to reduce residual risk is not the best recommendation, because it may not be feasible, efficient, or sufficient to address the risk and the control deterioration. Compensating controls are additional or alternative controls that are implemented to mitigate the risk when the primary control is not available, adequate, or effective. However, implementing compensating controls without discussing with the risk owner may result in wasting resources, duplicating efforts, or conflicting objectives, and may not align with the risk appetite or strategy of the organization.
B). Escalate the issue to senior management is not the best recommendation, because it may not be necessary, timely, or appropriate to involve senior management in the risk and control deterioration issue. Senior management is the highest level of authority and oversight in the organization, and may not have the detailed or operational knowledge or involvement in the risk and control management. Escalating the issue to senior management without discussing with the risk owner may create confusion, delay, or misunderstanding, and may not result in the optimal risk mitigation solution.
D). Certify the control after documenting the concern is not the best recommendation, because it may not be accurate, honest, or compliant to certify the control when it has deteriorated over time. Certifying the control is the process of attesting that the control is designed and operating effectively and efficiently, and meets the established criteria and standards. Certifying the control after documenting the concern may not reflect the true status and performance of the control, and may not comply with the internal or external audit or regulatory requirements. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 115. Roles and Responsibilities in Risk Management, Risk Owner vs. Control Owner: What's the Difference?, Control Deterioration: How to Avoid It and What to Do About It

NEW QUESTION: 90

Which of the following would MOST effectively reduce the potential for inappropriate exposure of vulnerabilities documented in an organization's risk register?

Freecram.net

A. Limit access to senior management only.
B. Encrypt the risk register.
C. Implement role-based access.
D. Require users to sign a confidentiality agreement.
Answer: (SHOW ANSWER)
A risk register is a document that contains information about potential cybersecurity risks that could threaten a project's success, or even the business itself2. Therefore, it is important to protect the confidentiality and integrity of the risk register from unauthorized or inappropriate access, modification, or disclosure. One way to do this is to implement role-based access, which is a method of restricting access to the risk register based on the roles or responsibilities of the users1. This way, only authorized users who need to view or edit the risk register for legitimate purposes can do so, and the access rights can be revoked or modified as needed. This would most effectively reduce the potential for inappropriate exposure of vulnerabilities documented in the risk register. The other options are not as effective or feasible as option C, as they do not address the need to balance the security and availability of the risk register. Option A, limiting access to senior management only, would compromise the availability and usefulness of the risk register, as other

stakeholders such as project managers, risk owners, or auditors may need to access the risk register for risk identification, analysis, response, or monitoring purposes3. Option B, encrypting the risk register, would enhance the security of the risk register, but it would not prevent authorized users from exposing the vulnerabilities to unauthorized parties, either intentionally or unintentionally. Encryption also adds complexity and cost to the risk register management process, and may affect the performance or usability of the risk register4. Option D, requiring users to sign a confidentiality agreement, would rely on the compliance and ethics of the users, but it would not prevent or detect any breaches of the agreement. A confidentiality agreement also does not specify the access rights or roles of the users, and may not be legally enforceable in some cases5.

NEW QUESTION: 91
While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:
A. control is ineffective and should be strengthened
B. risk is inefficiently controlled.
C. risk is efficiently controlled.
D. control is weak and should be removed.
Answer: (SHOW ANSWER)
Risk is inefficiently controlled when the annual cost of the control exceeds the annual loss expectancy (ALE) of the risk, as this means that the organization is spending more on the control than the potential loss that the control is supposed to prevent or reduce. This indicates that the control is not cost-effective or optimal, and that the organization should consider alternative or complementary controls that can lower the cost or increase the benefit of the risk management. Control is ineffective and should be strengthened when the control does not reduce the likelihood or impact of the risk to an acceptable level, regardless of the cost. Risk is efficiently controlled when the annual cost of the control is equal to or less than the annual loss expectancy (ALE) of the risk, as this means that the organization is spending less or equal on the control than the potential loss that the control is supposed to prevent or reduce. Control is weak and should be removed when the control does not provide any benefit or value to the risk management, regardless of the cost. References = CRISC Certified in Risk and Information Systems Control - Question205; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 205.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
Which of the following is the MOST important consideration when selecting digital signature software?

A. Availability
B. Nonrepudiation
C. Accuracy
D. Completeness
Answer: (SHOW ANSWER)
Digital Signature Software:
Digital signatures are used to verify the authenticity and integrity of a message, document, or software. They provide cryptographic proof that the information has not been altered and that it comes from a verified source.
Importance of Nonrepudiation:
Nonrepudiation ensures that the sender of the message cannot deny having sent the message and the recipient cannot deny having received it. This is critical for legal and security purposes, as it provides undeniable proof of the origin and integrity of the information.
Selecting Digital Signature Software:
When selecting digital signature software, the most important consideration is that it provides strong nonrepudiation capabilities. This ensures that all parties involved can trust the authenticity and integrity of the signed data.
Comparing Other Considerations:
Availability:Ensures the software is accessible when needed but does not directly impact the trustworthiness of the signatures.
Accuracy:Important but generally inherent in properly functioning digital signature software.
Completeness:Ensures all required information is included but nonrepudiation is the critical factor for security and legal purposes.
References:
The CISSP Study Guide emphasizes the importance of nonrepudiation in digital signature technology to ensure authenticity and accountability (Sybex CISSP Study Guide, Chapter 7: PKI and Cryptographic Applications).

NEW QUESTION: 93
Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?
A. A robust risk aggregation tool set
B. Clearly defined roles and responsibilities
C. A well-established risk management committee
D. Well-documented and communicated escalation procedures
Answer: (SHOW ANSWER)
The most important foundational element of an effective three lines of defense model for an organization is clearly defined roles and responsibilities. The three lines of defense model is a framework that outlinesthe roles and responsibilities of different functions or groups within the organization in relation to risk management and internal control1. The three lines of defense are:

The first line of defense, which consists of the operational management and staff who own and manage the risks associated with their activities and processes. They are responsible for identifying, assessing, and mitigating the risks, as well as designing, implementing, and operating the controls.
The second line of defense, which consists of the specialized functions or units that provide oversight, guidance, and support to the first line of defense in managing the risks and controls. They are responsible for developing and maintaining the risk management framework, policies, and standards, as well as monitoring and reporting on the risk and control performance.
The third line of defense, which consists of the internal audit function that provides independent and objective assurance on the effectiveness and efficiency of the risk management and internal control system. They are responsible for evaluating and testing the design and operation of the risks and controls, as well as reporting and recommending improvements to the seniormanagement and the board. Clearly defined roles and responsibilities are essential for ensuring that the three lines of defense model works effectively and efficiently. They help to avoid confusion, duplication, or gaps in the risk management and internal control activities, as well as to ensure accountability, coordination, and communication among the different functions or groups. They also help to establish the appropriate level of independence, authority, and competence for each line of defense, as well as to align the risk management and internal control objectives and strategies with the organization's goals and values2. The other options are not the most important foundational element of an effective three lines of defense model for an organization, as they are either less relevant or less specific than clearly defined roles and responsibilities. A robust risk aggregation tool set is a set of methods or techniques that enable the organization to collect, consolidate, and analyze the risk data and information from different sources, levels, or perspectives. A robust risk aggregation tool set can help to enhance the risk identification, assessment, and reporting processes, as well as to support the risk decision making and prioritization. However, a robust risk aggregationtool set is not the most important foundational element of an effective three lines of defense model for an organization, as it does not address the roles and responsibilities of the different functions or groups in relation to risk management and internal control. A well-established risk management committee is a group of senior executives or managers who are responsible for overseeing and directing the risk management activities and performance of the organization. A well-established risk management committee can help to ensure the alignment and integration of the risk management objectives and strategies with the organization's goals and values, as well as to provide guidance and support to the different functions or groups involved in risk management and internal control. However, a well-established risk management committee is not the most important foundational element of an effective three lines of defense model for an organization, as it does not cover theroles and responsibilities of the operational management and staff, the specialized functions or units, or the internal audit function. Well-documented and communicated escalation procedures are the steps or actions that are taken to report and resolve any issues or incidents that may affect the risk management and internal control activities or performance of the organization. Well-documented and communicated escalation procedures can help to ensure the timely and appropriate response and resolution of the issues or incidents, as well as to inform and involve the relevant stakeholders and authorities. However, well-documented and communicated escalation procedures are not the most important foundational element of an effective three lines of defense model for an organization, as they do not define the roles and responsibilities of the different

functions or groups in relation to risk management and internal control. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter
3, Section 3.1.1, Page 85.

NEW QUESTION: 94
Which of the following is the MOST appropriate key control indicator (KCI) to help an organization prevent successful cyber risk events on the external-facing infrastructure?
A. Increasing number of threat actors
B. Increasing number of intrusion detection system (IDS) false positive alerts
C. Increasing percentage of unpatched demilitarized zone (DMZ) servers
D. Increasing trend of perimeter attacks
Answer: (SHOW ANSWER)
The percentage of unpatched DMZ servers is a critical KCI for preventing cyber risk events on external-facing infrastructure. Unpatched servers are vulnerable to exploitation, and monitoring this indicator helps ensure timely application of security updates, reducing the risk of successful attacks.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Key Control Indicators.

NEW QUESTION: 95
Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?
A. Audit engagement letter
B. Risk profile
C. IT risk register
D. Change control documentation
Answer: (SHOW ANSWER)
An IT risk register is a document that records and tracks the IT risks that have been identified and assessed by the risk practitioner. It contains information such as the risk description, the risk owner, the risk level, the risk response, the risk status, and the risk monitoring and reporting activities. An IT risk register is a dynamic document that needs to be updated regularly to reflect the changes in the IT environment and the risk landscape. When a software upgrade renders an existing key control ineffective, the risk practitioner should update the IT risk register to indicate the new risk level, the new risk response, and the new risk monitoring and reporting activities. This will ensure that the IT risk register remains accurate, relevant, and useful for IT risk management. Updating the IT risk register is more important than updating the audit engagement letter, the risk profile, or the change control documentation, because the IT risk register is the primary source of information and guidance for managing IT risks. The audit engagement letter is a formal agreement between the auditor and the auditee that defines the scope, objectives, and terms of the audit. The risk profile is a summary of the organization's risk appetite, risk tolerance, and risk exposure. The change control documentation is a record of the changes that have been made to the IT systems and processes. These documents are important for IT risk management, but they are not as critical as the IT risk register for

updating when a key control becomes ineffective. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.4: Risk Register, pp. 69-711

NEW QUESTION: 96
The MOST essential content to include in an IT risk awareness program is how to:
A. define the IT risk framework for the organization
B. populate risk register entries and build a risk profile for management reporting
C. comply with the organization's IT risk and information security policies
D. prioritize IT-related actions by considering risk appetite and risk tolerance
Answer: (SHOW ANSWER)
An IT risk awareness program shouldprimarily ensure that employees and stakeholders understand and comply with the organization's risk and information security policies. ISACA highlights that an awareness program must reinforce policy understanding to drive compliant and secure behavior across the organization.

NEW QUESTION: 97
The PRIMARY purpose of IT control status reporting is to:
A. ensure compliance with IT governance strategy.
B. assist internal audit in evaluating and initiating remediation efforts.
C. benchmark IT controls with Industry standards.
D. facilitate the comparison of the current and desired states.
Answer: (SHOW ANSWER)
IT control status reporting is the process of collecting and analyzing data about the effectiveness and efficiency of IT controls. IT controls are the policies, procedures, and practices that ensure the confidentiality, integrity, and availability of IT resources and information. IT control status reporting helps to monitor the performance of IT controls against the predefined objectives and criteria, and to identify any gaps or issues that need to be addressed. IT control status reporting also provides information to the stakeholders about the current status and progress of IT control implementation and improvement.
The primary purpose of IT control status reporting is to facilitate the comparison of the current and desired states of IT controls. This means that IT control status reporting helps to evaluate the gap between the actual and expected performance of IT controls, and to determine the actions and resources needed to close the gap.
IT control status reporting also helps to align the IT controls with the business goals and strategies, and to ensure that the IT controls are delivering value to the organization. By comparing the current and desired states of IT controls, IT control status reporting enables continuous improvement and optimization of IT control processes and outcomes.
The other options are not the primary purpose of IT control status reporting, but rather some of the benefits or outcomes of it. IT control status reporting can help to ensure compliance with IT governance strategy,but it is not the main reason for doing it. IT governance is the framework that defines the roles, responsibilities, and relationships among the stakeholders involved in IT decision making and oversight. IT control status reporting can support IT governance by providing relevant and reliable information to the stakeholders, and by demonstrating the accountability and transparency of IT control activities. However, IT control status

reporting is not the same as IT governance, and it is not the only way to ensure compliance with IT governance strategy.
IT control status reporting can also assist internal audit in evaluating and initiating remediation efforts, but it is not the main objective of it. Internal audit is an independent and objective assurance and consulting activity that evaluates the adequacy and effectiveness of IT controls, and provides recommendations for improvement.
IT control status reporting can provide input and evidence to the internal audit process, and help to identify the areas of IT control that need further review or testing. IT control status reporting can also help to monitor and track the implementation of the audit findings and recommendations, and to verify the results of the remediation efforts. However, IT control status reporting is not the same as internal audit, and it is not the only source of information for internal audit.
Finally, IT control status reporting can benchmark IT controls with industry standards, but it is not the main goal of it. Industry standards are the best practices or guidelines that define the minimum requirements or expectations for IT control performance and quality. IT control status reporting can help to compare the IT controls with the industry standards, and to identify the areas of IT control that need to be enhanced or updated. IT control status reporting can also help to demonstrate the compliance or conformance of IT controls with the industry standards, and to provide assurance to the external parties or regulators. However, IT control status reporting is not the same as industry standards, and it is not the only way to benchmark IT controls. References = Service Reporting in ITIL: Process, Objectives and Examples - KnowledgeHut Anatomy of an effective status report - Project Management Institute How to Create a Project Status Report [Template & Examples] Communicating Document Control Progress on a Project
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 98
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for:
A. data retention and destruction.
B. data logging and monitoring.
C. data classification and labeling.
D. data mining and analytics.
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Of the following, who is responsible for approval when a change in an application system is ready for release to production?
A. Information security officer
B. IT risk manager
C. Business owner
D. Chief risk officer (CRO)
Answer: (SHOW ANSWER)

The business owner is the person who is responsible for approval when a change in an application system is ready for release to production. The business owner is the person who has the authority and accountability for the business process or function that is supported by the application system. The business owner should approve the change to ensure that it meets the business requirements, objectives, and expectations, and that it does not introduce any adverse impacts or risks to the business operations. The information security officer, the IT risk manager, and the chief risk officer (CRO) are not responsible for the approval of the change, although they may provide input, feedback, or oversight. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.1, page 3-32.

NEW QUESTION: 100

When establishing an enterprise IT risk management program, it is MOST important to:

A. review alignment with the organizations strategy.

B. understand the organization's information security policy.

C. validate the organization's data classification scheme.

D. report identified IT risk scenarios to senior management.

Answer: (SHOW ANSWER)

The most important thing to do when establishing an enterprise IT risk management program is to review the alignment with the organization's strategy. The organization's strategy is the plan or direction that the organization follows to achieve its vision, mission, and goals. The IT risk management program should be aligned with the organization's strategy, so that it supports and enables the organization's strategic objectives, and addresses the IT risks that could affect the organization's performance and value. Reviewing the alignment with the organization's strategy helps to ensure that the IT risk management program is relevant, effective, and consistent with the organization's expectations and needs. The other options are not as important as reviewing the alignment with the organization's strategy, although they may be useful or necessary steps or components of the IT risk management program. Understanding the organization's information security policy, validating the organization's data classification scheme, and reporting identified IT risk scenarios to senior management are all activities that can help to implement and improve the IT risk management program, but they are not the initial or primary thing to do. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.1, page 2-12.

NEW QUESTION: 101

The percentage of unpatched systems is a:

A. threat vector.

B. critical success factor (CSF).

C. key performance indicator (KPI).

D. key risk indicator (KRI).

Answer: (SHOW ANSWER)

The percentage of unpatched systems is best classified as a Key Risk Indicator (KRI). KRIs are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the business. Here' s a Understanding KRIs:

Definition: KRIs are specific metrics that provide insights into the risk level of an organization. They help in identifying potential risks that could impact the business negatively if not addressed promptly.
Purpose: KRIs are used to monitor the effectiveness of risk management strategies and to provide an early warning system for emerging risks.
Percentage of Unpatched Systems as a KRI:
Indicator of Vulnerability: The percentage of unpatched systems directly indicates how vulnerable an organization is to cyber threats. Unpatched systems are a common entry point for attackers, making this metric critical for assessing the organization's exposure to cyber risks.
Impact on Security Posture: A high percentage of unpatched systems can significantly increase the likelihood of security incidents, making it a valuable metric for risk management.
Proactive Risk Management: By monitoring this KRI, organizations can take proactive measures to address vulnerabilities before they are exploited.
Comparison with Other Options:
Threat Vector: A threat vector refers to the path or means by which a threat can reach and impact an asset. It is not a metric like the percentage of unpatched systems.
Critical Success Factor (CSF): CSFs are essential elements necessary for an organization to achieve its mission. While important, they are not specific metrics used to measure risk.
Key Performance Indicator (KPI): KPIs measure how effectively an organization is achieving its key business objectives. While related, KPIs focus on performance rather than risk exposure.
References:
CRISC Review Manual: Provides detailed insights into KRIs and their role in risk management.
ISACA Risk IT Framework: Discusses the use of KRIs in monitoring and managing IT risks effectively.

NEW QUESTION: 102
Which of the following should be considered FIRST when managing a risk event related to theft and disclosure of customer information?
A. Protecting the organization from negative publicity
B. Performing a root cause analysis to prevent incident recurrence
C. Containing the impact of the incident to affected customers
D. Preventing further dissemination of customer information
Answer: (SHOW ANSWER)
Thefirst stepis toprevent further disseminationof sensitive data to limit the impact of the breach. ISACA emphasizes that containment is the priority in risk response to minimize harm before addressing other aspects like root cause analysis or reputational management.

NEW QUESTION: 103
Which of the following scenarios is MOST likely to cause a risk practitioner to request a formal risk acceptance sign-off?
A. Residual risk in excess of the risk appetite cannot be mitigated.
B. Inherent risk is too high, resulting in the cancellation of an initiative.
C. Risk appetite has changed to align with organizational objectives.

D. Residual risk remains at the same level over time without further mitigation.

Answer: (SHOW ANSWER)

Requesting a formal risk acceptance sign-off is the most likely scenario when the residual risk in excess of the risk appetite cannot be mitigated, because it indicates that the organization is willing to tolerate a higher level of risk than it normally would, and that the risk owner has the authority and accountability to accept the risk and its consequences. Risk acceptance is a risk response strategy that involves acknowledging the existence of a risk and deciding not to take any action to reduce it. Risk acceptance is usually chosen when the cost or effort of mitigating the risk outweighs the potential benefits, or when no feasible mitigation options are available. Residual risk is the risk that remains after applying controls or mitigating factors. Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Inherent risk, cancellation of an initiative, change of risk appetite, and constant residual risk are all possible scenarios that may affect the risk management process, but they are not the most likely to cause a risk practitioner to request a formal risk acceptance sign-off, as they do not necessarily involve a risk owner accepting a higher level of risk than the organization's risk appetite. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.2, page 103

NEW QUESTION: 104

Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

A. Automated controls

B. Security awareness training

C. Multifactor authentication

D. Employee sanctions

Answer: (SHOW ANSWER)

The best control to reduce the likelihood of a successful network attack through social engineering is security awareness training. Security awareness training is a program that educates and trains employees on the common types, techniques, and indicators of social engineering attacks, such as phishing, baiting, pretexting, and quid pro quo12. Security awareness training also teaches employees how to protect themselves and the organization from social engineering attacks, such as by verifying the identity and legitimacy of the sender or caller, avoiding clicking on suspicious links or attachments, reporting any suspicious or unusual activity, and following the organization's security policies and procedures. Security awareness training can help to reduce the likelihood of a successful network attack through social engineering, because it can increase the employees' knowledge, skills, and confidence in recognizing and responding to social engineering attempts, and it can also foster a culture of security and responsibility among the employees. The other options are not the best control, although they may be useful or complementary to security awareness training. Automated controls are technical or procedural controls that are performed by a system or a device without human intervention, such as firewalls, antivirus software, encryption, and backups. Automated controls can help to protect the network from external or internal threats, but they may not be effective against social engineering attacks, which rely on human interaction and manipulation. Multifactor authentication is a security mechanism that requires users to provide two or more pieces of evidence to verify their identity and access a system or a service, such as a password, a token, a

fingerprint, or a facial recognition. Multifactor authentication can help to prevent unauthorized access to the network, but it may not prevent social engineering attacks, which may persuade users to share or compromise their authentication factors. Employee sanctions are disciplinary actions that are taken against employees who violate the organization's security policies and procedures, such as warnings, fines, suspensions, or terminations. Employee sanctions can help to deter and punish employees who fall victim to or facilitate social engineering attacks, but they may not prevent or reduce the likelihood of social engineering attacks, and they may also create a negative or fearful work environment. References = Avoiding Social Engineering and Phishing Attacks | CISA, What is Social Engineering | Attack Techniques & Prevention Methods ..., 10 Types of Social Engineering Attacks - CrowdStrike

NEW QUESTION: 105
An engineer has been assigned to conduct data restoration after a server storage failure. However, the procedure was not successful. Which of the following is the MOST probable cause of this situation?
A. Failure to test the disaster recovery plan (DRP)
B. Failure to prepare a business continuity plan (BCP)
C. Insufficient data captured in the business impact analysis (BIA)
D. Insufficient definition of the recovery point objective (RPO)
Answer: (SHOW ANSWER)
The RPO defines how much data loss is acceptable during system failure. If not clearly defined, restoration may skip key data, leading to incomplete recovery. ISACA guidelines highlight that alignment of RPO/RTO with business objectives is critical for viable DR planning

NEW QUESTION: 106
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?
A. Obtain objective assessment of the control environment.
B. Ensure the risk profile is defined and communicated.
C. Validate the threat management process.
D. Obtain an objective view of process gaps and systemic errors.
Answer: (SHOW ANSWER)
The risk management process is the systematic and continuous process of identifying, analyzing, evaluating, and treating the risks that may affect the organization's objectives, operations, or assets1. The risk management process should be aligned with the organization's overall risk management framework and strategy, and support the organization's value creation and protection2.
Having the risk management process reviewed by a third party is a good practice that can provide various benefits for the organization, such as:
Enhancing the credibility and reliability of the risk management process and outcomes Identifying and addressing any weaknesses, gaps, or errors in the risk management process and controls Providing independent and objective feedback and recommendations for improving the risk management process and performance Ensuring compliance with the relevant laws, regulations, and standards for risk management3
Among the four options given, the primary reason to have the risk management process reviewed by a third

party is to obtain an objective view of process gaps and systemic errors. This means that the third party can help to:
Assess the adequacy and effectiveness of the risk management process and its alignment with the organization's risk appetite and tolerance Detect and report any inconsistencies, inefficiencies, or inaccuracies in the risk identification, analysis, evaluation, or treatment activities Identify and prioritize the root causes and consequences of the process gaps and systemic errors, and their impact on the organization's risk exposure and acceptance Suggest and implement corrective or preventive actions that can resolve or mitigate the process gaps and systemic errors, and prevent their recurrence References = Risk Management Process - ISO 31000, Enterprise Risk Management - Wikipedia, How to Select a Third-Party Risk Management Framework

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
A risk practitioner implemented a process to notify management of emergency changes that may not be approved. Which of the following is the BEST way to provide this information to management?
A. Change logs
B. Change management meeting minutes
C. Key control indicators (KCIs)
D. Key risk indicators (KRIs)
Answer: (SHOW ANSWER)
The best way to provide information to management about emergency changes that may not be approved is to use key risk indicators (KRIs). KRIs are metrics that measure the likelihood and impact of risks, and help monitor and prioritize the most critical risks. KRIs help to provide information to management about emergency changes, because they help to alert and inform management about the potential risks and consequences of the changes, and to support the risk decision-making and reporting processes. KRIs also help to provide information to management about emergency changes, because they help to track and evaluate the effectiveness and performance of the changes, and to identify and address any issues or gaps that may arise from the changes. The other options are not the best way to provide information to management about emergency changes, although they may be part of or derived from the KRIs. Change logs, change management meeting minutes, and key control indicators (KCIs) are all examples of documentation or communication tools, which may help to record or report the details and status of the changes, but they do not necessarily measure or monitor the risks and outcomes of the changes. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.5.1, page 4-38.

NEW QUESTION: 108
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?
A. Sufficient resources are not assigned to IT development projects.
B. Customer support help desk staff does not have adequate training.
C. Email infrastructure does not have proper rollback plans.
D. The corporate email system does not identify and store phishing emails.
Answer: (SHOW ANSWER)
In an environment where reduced time-to-market for new software products is a top business priority, the risk practitioner's greatest concern should be whether sufficient resources are assigned to IT development projects.
Resources include human, financial, technical, and physical assets that are needed to plan, design, develop, test, and deliver high-quality software products in a timely manner. If the IT development projects are under-resourced, they may face challenges such as delays, errors, defects, rework, scope creep, or failure to meet customer expectations or requirements. These challenges can increase the risk of losing competitive advantage, market share, customer satisfaction, or reputation. The other options are less critical, as they are not directly related to the core business priority of reducing time-to-market for new software products. Customer support help desk staff training, email infrastructure rollback plans, and corporate email system phishing detection are important aspects of information security and customer service, but they are not the primary drivers of software product development and delivery. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.2: Risk Response Options, p. 115-116.

NEW QUESTION: 109
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?
A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.
Answer: (SHOW ANSWER)
The best course of action for the risk practitioner who has identified that the agreed RTO with a SaaS provider is longer than the business expectation is to document the gap in the risk register and report to senior management. The risk register is the document that records the details of all identified risks, including their sources, causes, impacts, likelihood, and responses. The risk register should be updated regularly to reflect any changes in the risk environment or the risk status. Reporting to senior management is also important, because senior management is the highest level of authority and responsibility in the organization, and they are responsible for setting the strategic direction, objectives, and risk appetite of the organization. Senior management should also oversee the risk management process, and ensure that the risks are aligned with the organization's goals and values. By documenting the gap in the risk register and reporting to senior management, the risk practitioner can communicate the issue clearly and effectively, and seek

guidance and support for resolving the problem. Collaborating with the risk owner, including a right to audit clause, or advising the risk owner to accept the risk are not the best courses of action, because they may not be feasible, effective, or desirable in some situations, or they may require senior management approval or involvement. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 110

Which of the following aspects of an IT risk and control self-assessment would be MOST important to include in a report to senior management?

Freecram.net

A. Changes in control design

B. A decrease in the number of key controls

C. Changes in control ownership

D. An increase in residual risk

Answer: (SHOW ANSWER)

An IT risk and control self-assessment (RCSA) is a process that helps organizations identify and evaluate operational risks and assess the effectiveness of their control measures12. It is a structured approach that involves identifying, assessing, mitigating, and monitoring risks across all levels of an organization12.

A report to senior management is a document that summarizes and communicates the results and findings of the RCSA, and provides recommendations and action plans for improving the risk management and control processes34.

The most important aspect of an IT risk and control self-assessment to include in a report to senior management is an increase in residual risk, which is the risk remaining after risk treatment, and represents the exposure or potential impact of the risk on the organization's objectives56.

An increase in residual risk is the most important aspect because it indicates the level of risk that the organization is willing to accept or tolerate, and the gap between the current and desired risk profile56.

An increase in residual risk is also the most important aspect because it requires the attention and decision of the senior management, who are responsible for defining the organization's risk appetite, strategy, and criteria, and for ensuring that the residual risk is within the acceptable range56.

The other options are not the most important aspects, but rather possible components or outcomes of an IT risk and control self-assessment that may support or complement the report to senior management. For example:

Changes in control design are components of an IT risk and control self-assessment that involve modifying or updating the control measures to address the changes in the risk environment or the organization's objectives56. However, changes in control design are not the most important aspect because they do not measure or reflect the residual risk, which is the ultimate goal of the risk treatment56.

A decrease in the number of key controls is an outcome of an IT risk and control self-assessment that indicates the improvement or optimization of the control processes, and the reduction of the complexity or redundancy of the control measures56. However, a decrease in the number of key controls is not the most important aspect because it does not indicate or imply the residual risk, which may depend on other factors such as the effectiveness or efficiency of the controls56.

Changes in control ownership are components of an IT risk and control self-assessment that involve assigning or reassigning the responsibility and accountability for the control processes to the appropriate individuals or groups within the organization56. However,changes in control ownership are not the most important aspect because they do not affect or determine the residual risk, which is independent of the control owners56. References =
1: Risk and control self-assessment - KPMG Global1
2: Control Self Assessments - PwC2
3: How-To Guide: Implementing Risk Control Self-Assessment Steps4
4: RISK MANAGEMENT SELF-ASSESSMENT TEMPLATE - Smartsheet5
5: Risk IT Framework, ISACA, 2009
6: IT Risk Management Framework, University of Toronto, 2017

NEW QUESTION: 111
Which of the following is the BEST indicator of an effective IT security awareness program?
A. Decreased success rate of internal phishing tests
B. Decreased number of reported security incidents
C. Number of disciplinary actions issued for security violations
D. Number of employees that complete security training
Answer: (SHOW ANSWER)
The best indicator of an effective IT security awareness program is the decreased success rate of internal phishing tests. Phishing is a type of social engineering attack that attempts to trick the users into revealing their personal or confidential information, or clicking on malicious links or attachments, by impersonating a legitimate entity or person. Internal phishing tests are simulated phishing attacks that are conducted by the enterprise to test the awareness and behavior of the employees in response to phishing emails. A decreased success rate of internal phishing tests means that fewer employees fall victim to the phishing attempts, and that they are more aware and vigilant of the phishing threats and techniques. A decreased success rate of internal phishing tests also implies that the IT security awareness program has effectively educated and trained the employees on how to recognize and report phishing emails, and how to protect themselves and the enterprise from phishing attacks. A decreased number of reported security incidents, a number of disciplinary actions issued for security violations, and a number of employees that complete security training are not as good indicators of an effective IT security awareness program as a decreased success rate of internal phishing tests, as they do not directly measure the awareness and behavior of the employees in relation to phishing, and may be influenced by other factors such as reporting mechanisms, enforcement policies, and training availability. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 220.

NEW QUESTION: 112
Who is ULTIMATELY accountable for risk treatment?
A. Risk owner
B. Enterprise risk management (ERM)
C. Risk practitioner
D. Control owner

Answer: (SHOW ANSWER)
The risk owner holds ultimate accountability for risk treatment, as they are responsible for decisions regarding the management and mitigation of the risk. This is a fundamental principle of Risk Ownership and Accountability within the CRISC framework.

NEW QUESTION: 113
Before selecting a final risk response option for a given risk scenario, management should FIRST:
A. determine control ownership.
B. determine the remediation timeline.
C. evaluate the organization's ability to implement the solution.
D. evaluate the risk response of similar sized organizations.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Recovery the objectives (RTOs) should be based on
A. minimum tolerable downtime
B. minimum tolerable loss of data.
C. maximum tolerable downtime.
D. maximum tolerable loss of data
Answer: (SHOW ANSWER)
Recovery time objectives (RTOs) are the acceptable timeframes within which business processes must be restored after a disruption. RTOs should be based on the maximum tolerable downtime (MTD), which is the longest time that a business process can be inoperable without causing irreparable harm to the organization. The other options are not directly related to RTOs, as they refer to the amount of data loss or corruption that can be tolerated, not the time to restore the business processes. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.3: Key Risk Indicators, page 197.

NEW QUESTION: 115
Which of the following will BEST quantify the risk associated with malicious users in an organization?
A. Business impact analysis
B. Risk analysis
C. Threat risk assessment
D. Vulnerability assessment
Answer: (SHOW ANSWER)
A threat risk assessment will best quantify the risk associated with malicious users in an organization, because it focuses on identifying and evaluating the potential sources of harm or damage to the organization's assets, such as data, systems, or networks. A malicious user is a person who intentionally and unauthorizedly accesses, modifies, destroys, or steals the organization's information or resources, for personal gain, revenge, espionage, or sabotage. A threat risk assessment can help the organization to estimate the likelihood and impact of malicious user attacks, based on factors such as the user's motivation,

capability, opportunity, and access level. A threat risk assessment can also help the organization to determine the appropriate risk response strategies, such as prevention, detection, mitigation, or transfer, to reduce the risk exposure and impact of malicious user attacks. References = Risk IT Framework, ISACA, 2022, p. 141

NEW QUESTION: 116
After identifying new risk events during a project, the project manager s NEXT step should be to:
A. determine if the scenarios need 10 be accepted or responded to.
B. record the scenarios into the risk register.
C. continue with a qualitative risk analysis.
D. continue with a quantitative risk analysis.
Answer: (SHOW ANSWER)
After identifying new risk events during a project, the project manager's next step should be to record the scenarios into the risk register, which is a document that records and tracks the identified risks, their causes, impacts, likelihood, responses, owners, and status. Recording the scenarios into the risk register helps to document and communicate the risks to the project team and stakeholders, and to facilitate the subsequent risk analysis and response processes. The other options are not the next steps, but rather the subsequent steps after recording the scenarios into the risk register. Determining if the scenarios need to be accepted or responded to is part of the risk evaluation and treatment process, which requires a prior risk analysis. Continuing with a qualitative or quantitative risk analysis is part of the risk assessment process, which requires a prior risk identification and documentation. References = Risk Register: A Project Manager's Guide with Examples
[2023] * Asana; Risk Identification in Project Management; 6.3. The 5 Steps of the Risk Management Process

NEW QUESTION: 117
Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?
A. An IT project manager is not assigned to oversee development.
B. Controls are not applied to the applications.
C. There is a lack of technology recovery options.
D. The applications are not captured in the risk profile.
Answer: (SHOW ANSWER)
The GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs is:
B: Controls are not applied to the applications.
When end users create their own applications, there is often a lack of formal controls that would typically be applied in a structured development environment. This can lead to issues with data integrity, security vulnerabilities, and non-compliance with organizational policies and standards.

NEW QUESTION: 118

The MOST effective approach to prioritize risk scenarios is by:

A. assessing impact to the strategic plan.

B. aligning with industry best practices.

C. soliciting input from risk management experts.

D. evaluating the cost of risk response.

Answer: (SHOW ANSWER)

The most effective approach to prioritize risk scenarios is by assessing the impact to the strategic plan, because this will help to align the risk management process with the organization's vision, mission, and goals.

The strategic plan is the document that defines the organization's direction, priorities, and objectives, and guides the allocation of resources and efforts. By assessing the impact to the strategic plan, the organization can determine which risk scenarios pose the greatest threat or opportunity to the achievement of the strategic objectives, and prioritize them accordingly. The other options are not as effective as assessing the impact to the strategic plan, because they do not directly relate to the organization's specific context, needs, and expectations, as explained below:

B: Aligning with industry best practices is an approach that involves following the standards, norms, and expectations for risk management that are established and followed by the peers or competitors in the same industry or sector. Aligning with industry best practices can help to benchmark and compare the organization's risk management performance and maturity, and identify areas for improvement or innovation. However, this approach is not as effective as assessing the impact to the strategic plan, because it does not account for the organization's unique and customized risk scenarios, which may differ from the industry average or standard.

C: Soliciting input from risk management experts is an approach that involves seeking advice, guidance, or feedback from the professionals or specialists who have the knowledge, experience, or skills in risk management. Soliciting input from risk management experts can help to enhance the quality and validity of the risk analysis and evaluation, and provide insights and recommendations for risk mitigation. However, this approach is not as effective as assessing the impact to the strategic plan, because it does not reflect the organization's risk appetite, preferences, and expectations, which may differ from the risk management experts' opinions or perspectives.

D: Evaluating the cost of risk response is an approach that involves estimating the resources and efforts required to implement the risk response strategies, such as avoiding, reducing, transferring, or accepting the risk. Evaluating the cost of risk response can help to optimize the risk management efficiency and effectiveness, and balance the potential benefits and costs of taking risks. However, this approach is not as effective as assessing the impact to the strategic plan, because it does not consider the potential consequences and outcomes of the risk scenarios, which may affect the organization's performance and reputation. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.3.1, page

45. The Ultimate Guide to Risk Prioritization - Hyperproof, Risk Prioritization: What Is It? [2021 Guide & Matrix] - ERM Software, What is Risk Prioritization | Centraleyes, Scenario Planning in Risk Management: Why It is Needed - SmartCompliance

NEW QUESTION: 119
A systems interruption has been traced to a personal USB device plugged into the corporate network by an IT employee who bypassed internal control procedures. Of the following, who should be accountable?
A. Business continuity manager (BCM)
B. Human resources manager (HRM)
C. Chief risk officer (CRO)
D. Chief information officer (CIO)
Answer: (SHOW ANSWER)
A systems interruption caused by a personal USB device plugged into the corporate network by an IT employee who bypassed internal control procedures is a serious breach of information security and IT risk management. The person who should be accountable for this incident is the chief information officer (CIO), who is responsible for overseeing the IT function and ensuring compliance with IT policies and standards. The CIO should also ensure that appropriate corrective and preventive actions are taken to prevent such incidents from recurring and to mitigate the impact of the systems interruption on the business operations and objectives. The CIO should also report the incident to the senior management and the board of directors, and communicate with the relevant stakeholders about the incident and the actions taken. References = Risk IT Framework, ISACA, 2022, p. 181

NEW QUESTION: 120
An organization is outsourcing a key database to be hosted by an external service provider. Who is BEST suited to assess the impact of potential data loss?
Freecram.net
A. Database manager
B. Public relations manager
C. Data privacy manager
D. Business manager
Answer: (SHOW ANSWER)
The business manager is best suited to assess the impact of potential data loss when outsourcing a key database to an external service provider.
* Role of the Business Manager:
* Understanding Business Impact: The business manager has a comprehensive understanding of the business processes, the criticality of the data, and the potential impact of data loss on business operations.
* Decision Making: They are responsible for making decisions regarding risk tolerance, business continuity, and aligning the risk management practices with business objectives.
* Assessment of Data Loss Impact:
* Operational Impact: The business manager can evaluate how data loss would affect day-to-day operations and overall business continuity.
* Financial and Reputational Impact: They can also assess the financial repercussions and potential damage to the organization's reputation, providing a holistic view of the impact.
* References:
* The CRISC Review Manual highlights the importance of involving business managers in assessing the impact of data loss due to their understanding of business operations and strategic objectives .

NEW QUESTION: 121
An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?
A. Key control owner
B. Operational risk manager
C. Business process owner
D. Chief information security officer (CISO)
Answer: C (LEAVE A REPLY)
The business process owner is the person or entity that has the accountability and authority to manage a business process and its outcomes. The business process owner would be the most appropriate owner of the risk associated with an IT control gap in a key process, as they are responsible for ensuring that the process meets its objectives and delivers value to the enterprise. The business process owner should also ensure that the process is aligned with the enterprise's strategy and risk appetite, and that the process risks are identified, assessed, and mitigated effectively. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 247. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 247. CRISC Sample Questions 2024, Question 247. CRISC by Isaca Actual Free Exam Q&As, Question 9.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
When evaluating enterprise IT risk management it is MOST important to:
A. create new control processes to reduce identified IT risk scenarios
B. confirm the organization's risk appetite and tolerance
C. report identified IT risk scenarios to senior management
D. review alignment with the organization's investment plan
Answer: (SHOW ANSWER)
Enterprise IT risk management is the process of identifying, analyzing, evaluating, and treating the IT-related risks that may affect the organization's objectives, operations, or assets1. Enterprise IT risk management should be aligned with the organization's overall riskmanagement framework and strategy, and support the organization's value creation and protection2.
When evaluating enterprise IT risk management, it is most important to confirm the organization's risk appetite and tolerance. Risk appetite is the amount and type of risk that an organization is willing to take in order to meet its strategic objectives3. Risk tolerance is the acceptable level of variation that an organization

is willing to accept around its risk appetite4. By confirming the organization's risk appetite and tolerance, the evaluation can:
Ensure that the enterprise IT risk management is consistent and compatible with the organization's risk culture and vision Provide clear and measurable criteria and boundaries for assessing and prioritizing the IT risks and their impacts Guide the selection and implementation of the appropriate risk responses and controls that balance the costs and benefits of risk mitigation Enable the monitoring and reporting of the IT risk performance and outcomes, and the adjustment of the IT risk strategy and objectives as needed5 References = Enterprise IT Risk Management - ISACA, Enterprise Risk Management - Wikipedia, Risk Appetite - COSO, Risk Tolerance - COSO, Risk Appetite and Tolerance - IRM

NEW QUESTION: 123
Which of the following should be considered FIRST when assessing risk associated with the adoption of emerging technologies?
A. Organizational strategy
B. Cost-benefit analysis
C. Control self-assessment (CSA)
D. Business requirements
Answer: (SHOW ANSWER)
The first factor that should be considered when assessing risk associated with the adoption of emerging technologies is the organizational strategy. The organizational strategy defines the vision, mission, goals, and objectives of the enterprise, and provides the direction and guidance for its activities and decisions. The adoption of emerging technologies should be aligned with the organizational strategy, and support its achievement and performance. The organizational strategy also helps to determine the risk appetite and tolerance of the enterprise, and the criteria for evaluating the risks and benefits of the emerging technologies. Cost-benefit analysis, control self-assessment, and business requirements are also important factors to consider when assessing risk associated with the adoption of emerging technologies, but they are not the first factor to consider. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.2.1.1, page 181
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 656.

NEW QUESTION: 124
A business impact analysis (BIA) has documented the duration of maximum allowable outage for each of an organization's applications. Which of the following MUST be aligned with the maximum allowable outage?
A. Mean time to restore (MTTR)
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Mean time to detect (MTTD)
Answer: (SHOW ANSWER)
The recovery time objective (RTO) is the planned recovery time for a process or system which should occur before reaching the business process's maximum tolerable downtime (MTD) or maximum allowable outage

(MAO). The RTO must be aligned with the MAO to ensure that the continuity of the business process is not compromised by a prolonged outage. The RTO is determined by the business impact analysis (BIA) based on the criticality and urgency of the business process and its dependencies. The RTO also helps to select and implement appropriate recovery methods and procedures for the process or system. References = Risk and Information Systems Control Study Manual, Chapter 6: IT Risk Monitoring and Reporting, Section 6.2: ITRisk Reporting, Page 307; What is the difference between RPO, RTO, and MTD? - Tandem Blog.

NEW QUESTION: 125

Malware has recently affected an organization. The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:

A. a gap analysis

B. a root cause analysis.

C. an impact assessment.

D. a vulnerability assessment.

Answer: (SHOW ANSWER)

The most effective way to resolve the situation and define a comprehensive risk treatment plan would be to perform a root cause analysis. A root cause analysis is a method of identifying and addressing the underlying factors or causes that led to the occurrence of a problem or incident1. In this case, the problem or incident is the malware infection that affected the organization. By performing a root cause analysis, the organization can determine how and why the malware was able to infect the systems, what vulnerabilities or weaknesses were exploited, what controls or processes failed or were missing, and what actions or decisions contributed to the situation. A root cause analysis can help the organization to prevent or reduce the recurrence of similar incidents, as well as to improve the effectiveness and efficiency of the risk management process. A root cause analysis can also help the organization to define a comprehensive risk treatment plan, which is a set of actions or measures that are taken to modify the risk, such as reducing, avoiding, transferring, or accepting the risk2.

Based on the findings and recommendations of the root cause analysis, the organization can select and implement the most appropriate risk treatment option for the malware risk, as well as for any other related or emerging risks. The risk treatment plan should also include the roles and responsibilities, resources, timelines, and performance indicators for the risk treatment actions3. The other options are not the most effective ways to resolve the situation and define a comprehensive risk treatment plan, as they are either less thorough or less relevant than a root cause analysis. A gap analysis is a method of comparing the current state and the desired state of a process, system, or organization, and identifying the gaps or differences between them4. A gap analysis can help the organization to identify the areas of improvement or enhancement, as well as the opportunities or challenges for achieving the desired state. However, a gap analysis is not the most effective way to resolve the situation and define a comprehensive risk treatment plan, as it does not address the causes or consequences of the malware infection, or the actions or measures to mitigate the risk. An impact assessment is a method of estimating the potential effects or consequences of a change, decision, or action on a process, system, or organization5. An impact assessment can help the organization to evaluate the benefits and costs, as well as the risks and opportunities, of a proposed or implemented change, decision, or action.

However, an impact assessment is not the most effective way to resolve the situation and define a comprehensive risk treatment plan, as it does not investigate the origin or nature of the malware infection, or the solutions or alternatives to manage the risk. A vulnerability assessment is a method of identifying and analyzing the weaknesses or flaws in a process, system, or organization that can be exploited by threats to cause harm or loss6. A vulnerability assessment can help the organization to discover and prioritize the vulnerabilities, as well as to recommend and implement the controls or measures to reduce or eliminate them.
However, a vulnerability assessment is not the most effective way to resolve the situation and define a comprehensive risk treatment plan, as it does not consider the root causes or impacts of the malware infection, or the risk treatment options or plans to address the risk. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.8, Page 61.

NEW QUESTION: 126
An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?
A. Reduced ability to evaluate key risk indicators (KRIs)
B. Reduced access to internal audit reports
C. Dependency on the vendor's key performance indicators (KPIs)
D. Dependency on service level agreements (SLAs)
Answer: (SHOW ANSWER)
Reduced ability to evaluate key risk indicators (KRIs) will have the greatest impact on the ability to monitor risk when an information system for a key business operation is moved from an in-house application to a Software as a Service (SaaS) vendor, as it may limit the visibility and control over the risk exposure and performance of the system. KRIs are metrics that measure the level of risk exposure and the effectiveness of risk response strategies, and they should be aligned with the enterprise's risk appetite and objectives. When the system is moved to a SaaS vendor, the enterprise may lose access to the data and processes that are used to calculate and report the KRIs, or the KRIs may become irrelevant or inconsistent with the vendor's environment and standards. This may impair the ability to monitor risk and to take timely and appropriate actions to manage risk. Reduced access to internal audit reports, dependency on the vendor's key performance indicators (KPIs), and dependency on service level agreements (SLAs) are not the greatest impacts on the ability to monitor risk, as they do not affect the measurement and reporting of the risk status and performance, but rather the assurance and evaluation of the system quality and reliability. References = CRISC Certified in Risk and Information Systems Control - Question221; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 221.

NEW QUESTION: 127
Which of the following criteria for assigning owners to IT risk scenarios provides the GREATEST benefit to an organization?
A. The risk owner understands the effect of loss events on business operations.
B. The risk owner is a member of senior leadership in the IT organization.

C. The risk owner has strong technical aptitude across multiple business systems.
D. The risk owner has extensive risk management experience.
Answer: (SHOW ANSWER)
The risk owner should be someone who has the authority, responsibility, and knowledge to manage the risk effectively and align it with the organizational strategy and objectives. The risk owner should also be able to communicate the impact of the risk on the business operations and the value proposition of the risk response.
Understanding the effect of loss events on business operations is a key criterion for assigning risk owners, as it helps to prioritize and mitigate the risks that matter most to the organization.
References
*Why Assigning a Risk Owner is Important and How to Do It Right
*How to Write Strong Risk Scenarios and Statements - ISACA
*What Everybody Ought To Know About Project Risk Owners

NEW QUESTION: 128
Which of the following would BEST enable a risk practitioner to embed risk management within the organization?
A. Provide risk management feedback to key stakeholders.
B. Collect and analyze risk data for report generation.
C. Monitor and prioritize risk data according to the heat map.
D. Engage key stakeholders in risk management practices.
Answer: (SHOW ANSWER)
* Engaging key stakeholders in risk management practices is the best way to embed risk management within the organization. This means that the risk practitioner involves and communicates with the people who have an interest or influence in the organization's objectives, activities, and risks, such as senior management, business unit managers, employees, customers, suppliers, regulators, etc.
* Engaging key stakeholders in risk management practices helps to create a risk-aware culture, align risk management with the organization's strategy and vision, ensure the ownership and accountability of risks and controls, obtain the support and commitment for risk management initiatives, and improve the risk management performance and outcomes.
* The other options are not the best ways to embed risk management within the organization. They are either secondary or not essential for risk management.
The references for this answer are:
* Risk IT Framework, page 17
* Information Technology & Security, page 11
* Risk Scenarios Starter Pack, page 9

NEW QUESTION: 129
Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?
A. High percentage of lagging indicators
B. Nonexistent benchmark analysis

C. Incomplete documentation for KRI monitoring
D. Ineffective methods to assess risk
Answer: (SHOW ANSWER)
The greatest concern when establishing key risk indicators (KRIs) is using ineffective methods to assess risk. KRIs are metrics that measure the likelihood and impact of risks, and help monitor and prioritize the most critical risks. To establish effective KRIs, the risk assessment methods should be reliable, valid, consistent, and timely. Ineffective methods to assess risk could lead to inaccurate or misleading KRIs, which could result in poor risk management decisions and outcomes. The other options are not as significant as using ineffective methods to assess risk, although they may also affect the quality and usefulness of KRIs.
References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.4.1, page 4-36.

NEW QUESTION: 130
Which of the following is the PRIMARY purpose of conducting risk and control self-assessments?
A. To better understand inherent and residual risk within the organization
B. To gain objective insight into the effectiveness and efficiency of controls
C. To demonstrate compliance with regulatory and legal control requirements
D. To facilitate timely and accurate updates to the risk register
Answer: (SHOW ANSWER)
Risk and control self-assessments (RCSAs) are designed to helpbusiness units evaluate their own risks and controls, leading to a deeperunderstanding of inherent and residual riskand more accurate risk profiles.
Reference:CRISC Manual - Domain 4, Slide 392-395

NEW QUESTION: 131
Which of the following observations would be the GREATEST concern to a risk practitioner evaluating an organization's risk management practices?
A. Several risk scenarios have action plans spanning multiple years.
B. Business leaders provide final approval for information security policies.
C. Senior management has approved numerous requests for risk acceptance.
D. Senior management does not set risk tolerance.
Answer: (SHOW ANSWER)

NEW QUESTION: 132
When testing the security of an IT system, il is MOST important to ensure that;
A. tests are conducted after business hours.
B. operators are unaware of the test.
C. external experts execute the test.
D. agreement is obtained from stakeholders.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, stakeholders are the individuals or groups that have an interest or stake in the outcome of the IT system and its risks. Stakeholders include the system owners, users, operators, developers, managers, auditors, regulators, and customers. It is most important to ensure that

agreement is obtained from stakeholders when testing the security of an IT system, as this helps to define the scope, objectives, and expectations of the test, and to obtain the necessary authorization, support, and resources for the test. Agreement from stakeholders also helps to avoid any conflicts, disruptions, or misunderstandings that may arise during or after the test, and to ensure the validity and acceptance of the test results and recommendations. References = CRISC Review Manual1, page 198, 224.

NEW QUESTION: 133
Which of the following should be the GREATEST concern for an organization that uses open source software applications?
A. Lack of organizational policy regarding open source software
B. Lack of reliability associated with the use of open source software
C. Lack of monitoring over installation of open source software in the organization
D. Lack of professional support for open source software
Answer: (SHOW ANSWER)
Lack of organizational policy regarding open source software should be the greatest concern for an organization that uses open source software applications, as it may expose the organization to legal, security, and operational risks. Open source software is software that is freely available and can be modified and distributed by anyone, subject to certain conditions and licenses. An organizational policy regarding open source software should define the criteria and procedures for selecting, acquiring, using, and maintaining open source software, as well as the roles and responsibilities of the stakeholders involved. Lack of reliability, lack of monitoring, and lack of professional support are not the greatest concerns, as they can be addressed by implementing quality assurance, configuration management, and community engagement practices for open source software. References = CRISC by Isaca Actual Free Exam Q&As, question 214; CRISC: Certified in Risk & Information Systems Control Sample Questions, question 214.

NEW QUESTION: 134
When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important
A. revalidate current key risk indicators (KRIs).
B. revise risk management procedures.
C. review the data classification policy.
D. revalidate existing risk scenarios.
Answer: (SHOW ANSWER)
When developing a response plan to address security incidents regarding sensitive data loss, it is most important to review the data classification policy. A data classification policy is a document that defines the categories and levels of data based on their sensitivity, value, and criticality, and specifies the appropriate security measures and handling procedures for each data type. A data classification policy helps to identify and protect the sensitive data that could be exposed or compromised in a security incident, and to comply with the relevant laws, regulations, standards, and contracts. Reviewing the data classification policy is important when developing a response plan, because it helps to determine the scope, impact, and priority of the security incident, and to select the most appropriate and effective response actions and strategies.

Reviewing the data classification policy also helps to communicate and coordinate the response plan with the internal and external stakeholders, such as the data owners, users, custodians, and regulators, and to report and disclose the security incident as required. The other options are not as important as reviewing the data classification policy, although they may be part of or derived from the response plan. Revalidating current key risk indicators (KRIs), revising risk management procedures, and revalidating existing risk scenarios are all activities that can help to improve or update the risk management process, but they are not the most important when developing aresponse plan. References = Risk and Information Systems Control Study Manual, Chapter
5, Section 5.3.1, page 5-25.

NEW QUESTION: 135
Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?
A. Implementing record retention tools and techniques
B. Establishing e-discovery and data loss prevention (DLP)
C. Sending notifications when near storage quota
D. Implementing a bring your own device 1BVOD) policy
Answer: (SHOW ANSWER)
According to the Risk and Information Systems Control documents, implementing record retention tools and techniques is the best solution in this scenario. Record retention involves managing the lifecycle of records, including their creation, usage, storage, and disposal. By implementing record retention policies, organizations can define how long emails and other data should be retained before being deleted. This helps in efficiently managing storage space and reducing unnecessary storage costs.
Establishing e-discovery and data loss prevention (DLP) (Option B) focuses more on legal and compliance aspects and may not directly address the issue of reducing storage costs. Sending notifications when near storage quota (Option C) is a reactive approach and may not prevent the exponential increase in storage costs.
Implementing a bring your own device (BYOD) policy (Option D) is unrelated to the issue of email storage costs.
References = Risk and Information Systems Control Study Manual

NEW QUESTION: 136
Which of the following is the MOST important driver of an effective enterprise risk management (ERM) program?
A. Risk policy
B. Risk committee
C. Risk culture
D. Risk management plan
Answer: (SHOW ANSWER)

Risk culture is the foundation upon which ERM is built. It dictates how employees perceive, communicate, and act on risk. A strong risk culture ensures consistency in risk behaviors, supports governance, and sustains long-term effectiveness of the ERM.
Reference:CRISC Manual - Domain 1, Slide 80-84

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?
A. Updating the organizational policy for remote access
B. Creating metrics to track remote connections
C. Implementing multi-factor authentication
D. Updating remote desktop software
Answer: (SHOW ANSWER)
The management action that will most likely change the likelihood rating of a risk scenario related to remote network access is implementing multi-factor authentication. Multi-factor authentication is a technique that requires the user to provide two or more pieces of evidence to verify their identity, such as a password, a token, or a biometric factor. Multi-factor authentication can help to reduce the likelihood of unauthorized or malicious access to the remote network, as it adds an extra layer of security and makes it harder for the attackers to compromise the user credentials. The other options are not as likely to change the likelihood rating of the risk scenario, as they are related to the update, creation, or maintenance of the remote network access, not the verification or protection of the remote network access. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 138
What should a risk practitioner do FIRST upon learning a risk treatment owner has implemented a different control than what was specified in the IT risk action plan?
A. Seek approval from the control owner.
B. Update the action plan in the risk register.
C. Reassess the risk level associated with the new control.
D. Validate that the control has an established testing method.
Answer: (SHOW ANSWER)

The first thing that a risk practitioner should do upon learning that a risk treatment owner has implemented a different control than what was specified in the IT risk action plan is to reassess the risk level associated with the new control. This is because the new control may have a different effect on the likelihood and impact of the risk, and may introduce new risks or modify existing ones. The risk practitioner should evaluate the adequacy and effectiveness of the new control, and compare the residual risk with the risk appetite and tolerance of the organization. The risk practitioner should also communicate the results of the risk reassessment to the relevant stakeholders, and update the risk register and action plan accordingly. The other options are not the first things that a risk practitioner should do, although they may be necessary or appropriate at a later stage. Seeking approval from the control owner is important, but it does not address the potential changes in the risk level or the alignment with the risk management objectives. Updating the action plan in the risk register is a good practice, but it should be done after the risk reassessment and with the consent of the risk owner. Validating that the control has an established testing method is a part of the control assurance process, but it does not provide information on the risk level or the risk response effectiveness. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk Response, page 151.

NEW QUESTION: 139

A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

A. Risk appetite statement

B. Enterprise risk management framework

C. Risk management policies

D. Risk register

Answer: (SHOW ANSWER)

According to the CRISC Review Manual (Digital Version), the risk register is the most useful component of the review of the overall risk profile from the targeted organization, as it provides a comprehensive and up-to-date record of the identified risks, their likelihood and impact, their risk response actions, and their residual risk levels. The risk register helps to:

Understand the current and potential threats and vulnerabilities that may affect the targeted organization's objectives and performance Evaluate the effectiveness and efficiency of the risk management processes and controls implemented by the targeted organization Identify the gaps or weaknesses in the risk management practices and capabilities of the targeted organization Assess the compatibility and alignment of the risk appetite and risk tolerance of the targeted organization with the acquiring organization Estimate the value and benefits of the acquisition and the potential risks and costs involved References = CRISC Review Manual (Digital Version), Chapter 1: IT Risk Identification, Section 1.5: IT Risk Identification Methods and Techniques, pp. 38-391

NEW QUESTION: 140

A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?

Pdfcram.net

A. Conduct a gap analysis
B. Transfer risk to the third party
C. Terminate the outsourcing agreement
D. Identify compensating controls
Answer: (SHOW ANSWER)
When a new regulation affects outsourcing arrangements, the first and best response is to perform a gap analysis.
"Upon regulatory change, the risk practitioner should perform a gap analysis to determine areas of noncompliance and required updates in contracts or controls." Transferring or terminating agreements may follow depending on results.
Hence, A is correct.
CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Third-Party Risk and Compliance Management.

NEW QUESTION: 141
Why should an organization continually assess and improve its existing controls?
A. To gain stakeholder support for the implementation of controls
B. To address multiple risk scenarios mitigated by technical controls
C. To comply with industry best practices by balancing multiple types of controls
D. To improve the effectiveness of controls that mitigate risk
Answer: D (LEAVE A REPLY)
Administrative controls complement technical controls to enhance the overall effectiveness of risk mitigation. While technical controls implement the specific security mechanisms, administrative controls such as policies, procedures, and training ensure consistent and correct use of these technical controls, increasing their effectiveness in mitigating risk. This layered approach ensures that control measures are reinforced and integrated within the enterprise's risk management strategy.

NEW QUESTION: 142
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?
A. Develop a risk treatment plan.
B. Validate organizational risk appetite.
C. Review results of prior risk assessments.
D. Include the current and desired states in the risk register.
Answer: A (LEAVE A REPLY)
Developing a risk treatment plan is the best way to facilitate the mitigation of identified gaps between current and desired risk environment states. A risk treatment plan is a document that outlines the actions and resources needed to implement the chosen risk response strategy for each risk scenario. A risk treatment plan should include the following elements:
* Risk scenario description and risk ID
* Risk owner and other stakeholders

* Risk response strategy and objectives
* Risk response actions and tasks
* Resources, costs, and benefits
* Roles and responsibilities
* Timeline and milestones
* Performance indicators and monitoring mechanisms
* Contingency plans and triggers

A risk treatment plan helps to close the gaps between the current and desired risk environment states by providing a clear and comprehensive roadmap for risk mitigation. It also helps to ensure that the risk response actions are aligned with the organizational risk appetite, objectives, and priorities. A risk treatment plan also facilitates the communication, coordination, and collaboration among the risk owners and other stakeholders involved in the risk mitigation process.

The other options are not the best ways to facilitate the mitigation of identified gaps between current and desired risk environment states. Validating organizational risk appetite is an important step in establishing the risk criteria and thresholds for the risk assessment process, but it does not directly address the gaps between the current and desired risk environment states. Reviewing results of prior risk assessments can provide useful insights and lessons learned for the current risk assessment process, but it does not necessarily lead to the development and implementation of effective risk response actions. Including the current and desired states in the risk register can help to document and monitor the risk scenarios and their status, but it does not provide the details and guidance for risk mitigation. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4: Risk Response, Section 4.2: Risk Treatment, p. 189-191.

NEW QUESTION: 143

Which of the following is MOST important when defining controls?

A. Identifying monitoring mechanisms

B. Including them in the risk register

C. Aligning them with business objectives

D. Prototyping compensating controls

Answer: (SHOW ANSWER)

According to the CRISC Review Manual1, controls are the policies, procedures, practices, and organizational structures that are designed and implemented to manage risk. The most important factor when defining controls is to align them with the business objectives, as this helps to ensure that the controls support the achievement of the organization's strategy, goals, and values. Aligning controls with business objectives also helps to optimize the benefits and costs of controls, and to prioritize and allocate resources for control implementation and maintenance. References = CRISC Review Manual1, page 202.

NEW QUESTION: 144

Which of the following is the MAIN purpose of monitoring risk?

A. Communication

B. Risk analysis

C. Decision support
D. Benchmarking
Answer: (SHOW ANSWER)
The main purpose of monitoring risk is to provide decision support for the organization. Risk monitoring is the process of tracking and reviewing the risk management activities, the risk profile, and the risk performance of the organization. By monitoring risk, the organization can obtain timely and relevant information and feedback on the risk situation, and use it to make informed and effective decisions on risk management and business objectives. Communication, risk analysis, and benchmarking are other possible purposes of risk monitoring, but they are not as important as decision support. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 12; CRISC Review Manual, 6th Edition, page 215.

NEW QUESTION: 145
Which of the following is a KEY principle of a Zero Trust architecture?
A. Only allowing access to systems and data from trusted locations
B. Requiring periodic reauthentication of access to systems
C. Assuming that all systems are malicious
D. Mandating the use of complex passwords for access to data systems
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which of the following is the PRIMARY consideration when establishing an organization's risk management methodology?
A. Business context
B. Risk tolerance level
C. Resource requirements
D. Benchmarking information
Answer: (SHOW ANSWER)
The primary consideration when establishing an organization's risk management methodology is the business context, which includes the internal and external factors that influence the organization's objectives, strategies, scope, and boundaries. The business context helps to define the risk criteria, the risk appetite, the risk identification, the risk analysis, and the risk treatment. The other options are not the primary consideration, but rather the outcomes or inputs of the risk management methodology. References = ISO 31000 Risk Management - Principles and Guidelines; ISO 31000 Principles of Risk Management; The risk management process: What is the best structure and administration?

NEW QUESTION: 147
Which of the following is the MOST essential characteristic of a good IT risk scenario?
A. The scenario is aligned to business control processes.
B. The scenario is aligned to the organization's risk appetite and tolerance.
C. The scenario is aligned to a business objective.

D. The scenario is aligned to known vulnerabilities in information technology.

Answer: (SHOW ANSWER)

A good IT risk scenario must be aligned with a business objective. This alignment ensures that the risk scenario is relevant to the organization's goals and can be effectively integrated into its risk management processes.

Alignment to Business Objective (Answer C):

Importance: Aligning risk scenarios with business objectives ensures that they are relevant and support the organization's overall strategy.

Impact: This alignment helps in prioritizing risk management efforts and resources toward areas that directly affect the organization's success.

Outcome: It leads to more effective risk management by focusing on risks that could impact key business outcomes.

Comparison with Other Options:

A: The scenario is aligned to business control processes:

Purpose: Control processes are important but secondary to business objectives.

B: The scenario is aligned to the organization's risk appetite and tolerance:

Purpose: Important for overall risk management but not the primary characteristic of a good risk scenario.

D: The scenario is aligned to known vulnerabilities in information technology:

Purpose: While addressing vulnerabilities is important, the primary focus should be on how these vulnerabilities affect business objectives.

References:

ISACA CRISC Review Manual, Chapter 2, "IT Risk Assessment", which emphasizes the need for risk scenarios to be aligned with business objectives for effective risk management.

NEW QUESTION: 148

Risk appetite should be PRIMARILY driven by which of the following?

A. Enterprise security architecture roadmap

B. Stakeholder requirements

C. Legal and regulatory requirements

D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

Risk appetite should be primarily driven by stakeholder requirements. Stakeholder requirements are the needs and expectations of the internal and external parties that have an interest or influence in the organization's objectives or operations, such as the board, management, employees, customers, regulators, investors, etc.

Risk appetite is the amount and type of risk that the organization is willing to accept or pursue in order to achieve its objectives. Risk appetite should be driven by stakeholder requirements, because they reflect the organization's mission, vision, values, and strategy, and they provide the basis and direction for the organization's risk management activities. Risk appetite should also be aligned and communicated with stakeholder requirements, because they affect the organization's performance and reputation, and they require the organization's accountability and transparency. The other options are not the primary drivers of

risk appetite, although they may be considered or influenced by risk appetite. Enterprise security architecture roadmap, legal and regulatory requirements, and business impact analysis (BIA) are all factors that could affect the organization's risk profile, risk assessment, or risk response, but they do not necessarily determine or reflect the organization's risk appetite. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.3.1, page 2-23.

NEW QUESTION: 149

Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

A. Reject the risk acceptance and require mitigating controls.

B. Monitor the residual risk level of the accepted risk.

C. Escalate the risk decision to the project sponsor for review.

D. Document the risk decision in the project risk register.

Answer: (SHOW ANSWER)

Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk appetite can be expressed in qualitative or quantitative terms, and can vary depending on the context and the stakeholder. Risk appetite should be defined and communicated by the senior management or the board of directors, and should guide the risk management decisions and actions throughout the organization. When a project team has accepted a risk outside the established risk appetite, the risk practitioner's best course of action is to escalate the risk decision to the project sponsor for review, meaning that the risk practitioner should report the risk acceptance and its rationale to the project sponsor, who is the person or group that provides the resources and support for the project, and is accountable for its success. The project sponsor should review the risk decision and determine whether it is aligned with the organization's objectives and strategy, and whether it requires any further approval or action. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.1, p. 25-26

NEW QUESTION: 150

Which of the following actions should a risk practitioner do NEXT when an increased industry trend of external cyber attacks is identified?

Freecram.net

A. Conduct a threat and vulnerability analysis.

B. Notify senior management of the new risk scenario.

C. Update the risk impact rating in the risk register.

D. Update the key risk indicator (KRI) in the risk register.

Answer: A (LEAVE A REPLY)

A possible action that a risk practitioner should do next when an increased industry trend of external cyber attacks is identified is A. Conduct a threat and vulnerability analysis. A threat and vulnerability analysis is a process of identifying and assessing the potential sources and methods of cyber attacks, as well as the weaknesses and gaps in the organization's information systems and security controls12 By conducting a threat and vulnerability analysis, a risk practitioner can determine the level of exposure and risk that the organization faces from external cyber attacks, and prioritize the actions and resources needed to mitigate or prevent them3 A threat and vulnerability analysis can also help to update the risk impact rating and the key

risk indicator in the risk register, as well as to notify senior management of the new risk scenario, but these are subsequent steps that follow after the analysis is completed. Therefore, the first action that a risk practitioner should do next is to conduct a threat and vulnerability analysis.

NEW QUESTION: 151
An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?
A. Failure to test the disaster recovery plan (DRP)
B. Lack of well-documented business impact analysis (BIA)
C. Lack of annual updates to the disaster recovery plan (DRP)
D. Significant changes in management personnel
Answer: (SHOW ANSWER)
The most likely cause of the situation where the recovery team does not know what steps to take to recover critical data backups following a major flood is the failure to test the disaster recovery plan (DRP). A DRP is a document that describes the procedures and resources needed to restore the normal operations of an organization after a disaster. Testing the DRP is essential to ensure that the plan is feasible, effective, and up-to-date. Testing the DRP also helps to train the recovery team members, identify and resolve any issues or gaps, and improve the confidence and readiness of the organization. The lack of a well-documented business impact analysis (BIA), the lack of annual updates to the DRP, and the significant changes in management personnel are also possible factors that could affect the recovery process, but they are not as likely or as critical as the failure to test the DRP. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.3.1, page 5-19.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?
A. Number of times the recovery plan is reviewed
B. Number of successful recovery plan tests
C. Percentage of systems with outdated virus protection
D. Percentage of employees who can work remotely
Answer: (SHOW ANSWER)

A key control indicator (KCI) is a metric that provides information on the extent to which a given control is meeting its intended objectives in terms of loss prevention, reduction, etc. A KCI should have an explicit relationship to both the specific control and the specific risk against which the control has been implemented. For risk related to IT infrastructure failure, a possible control is to have a recovery plan that can restore the critical IT services and minimize the impact of the failure. A KCI that can measure the effectiveness of this control is the number of successful recovery plan tests, which indicates how well the recovery plan can be executed in a real scenario. The higher the number of successful tests, the lower the risk of IT infrastructure failure. Therefore, this is the best KCI among the given options. References = Integrating KRIs and KPIs for Effective Technology Risk Management Key Control Indicator (KCI) - CIO Wiki Infrastructure Issues: Understanding and Mitigating Risks

NEW QUESTION: 153
Which of the following information is MOST useful to a risk practitioner for developing IT risk scenarios?
A. Published vulnerabilities relevant to the business
B. Threat actors that can trigger events
C. Events that could potentially impact the business
D. IT assets requiring the greatest investment
Answer: (SHOW ANSWER)
Developing IT Risk Scenarios:
Risk scenarios are hypothetical events that describe potential threats and their impact on business operations.
These scenarios are essential for identifying and assessing risks.
Importance of Potential Impact Events:
Events that could potentially impact the business provide the most useful information for developing risk scenarios because they directly relate to the organization's objectives and operations.
Understanding these events helps in crafting realistic and relevant risk scenarios that can guide risk assessment and mitigation efforts.
Components of Risk Scenarios:
Threat Actors:Identify who might exploit vulnerabilities.
Threat Events:Describe the specific events that could impact the business.
Business Impact:Assess how these events would affect business operations, finances, reputation, etc.
Using Impact Events for Scenario Development:
Focusing on events that could disrupt critical business functions ensures that the scenarios are relevant and actionable.
It enables the risk practitioner to communicate the potential consequences effectively to stakeholders and prioritize mitigation efforts accordingly.
Comparing Other Information Sources:
Published Vulnerabilities:Useful for understanding specific threats but may not directly relate to business impact.
Threat Actors:Important for identifying potential sources of risk but not sufficient alone for scenario development.

IT Assets:Relevant for risk assessment but secondary to understanding potential impact events.
References:
The CRISC Review Manual discusses the importance of considering events that could impact the business when developing risk scenarios (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.4 Risk Scenario Development).

NEW QUESTION: 154
A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:
A. update the risk rating.
B. reevaluate inherent risk.
C. develop new risk scenarios.
D. implement additional controls.
Answer: (SHOW ANSWER)
The most important action for the risk practitioner to take when a risk assessment has identified increased losses associated with an IT risk scenario is to update the risk rating. A risk rating is a measure of the overall level of risk, based on the combination of the probability and impact of the risk scenario. A risk rating helps to prioritize the risks, communicate the risk exposure, and monitor the risk response. Updating the risk rating is the most important action, because it reflects the current state and magnitude of the risk, and it triggers the review and revision of the risk response plan, if needed. Updating the risk rating also ensures that the risk register and the risk profile are accurate and complete, and that the risk management process is consistent and effective. The other options are not the most important action, although they may be related or subsequent steps in the risk management process. Reevaluating inherent risk is a part of the risk analysis process, which estimates the probability and impact of the risk scenario before considering the existing controls.
Reevaluating inherent risk can help to identify the root causes and drivers of the risk, and to assess the effectiveness and efficiency of the controls, but it does not change the overall level of risk or the risk response plan. Developing new risk scenarios is a part of the risk identification process, which identifies and describes the potential events or situations that could affect the achievement of the objectives. Developing new risk scenarios can help to expand the scope and coverage of the risk management process, and to address the emerging or changing risks, but it does not update the existing risk scenarios or the risk response plan.
Implementing additional controls is a part of the risk response process, which selects and executes the appropriate actions to reduce, avoid, share, or exploit the risk. Implementing additional controls can help to mitigate the risk and achieve the desired risk level, but it is not the first or the only option, as it depends on the risk appetite, tolerance, and capacity of the organization, and the cost-benefit analysis of the controls.
References = Risk Register Template and Examples | Prioritize and Manage Risk, How to Write Strong Risk Scenarios and Statements - ISACA, IT Risk Resources | ISACA

NEW QUESTION: 155
Mitigating technology risk to acceptable levels should be based PRIMARILY upon:

A. organizational risk appetite.
B. business sector best practices.
C. business process requirements.
D. availability of automated solutions
Answer: (SHOW ANSWER)
Mitigating technology risk to acceptable levels means that the organization implements and maintains appropriate controls to reduce the likelihood and impact of potential threats or losses that may arise from the use of technology, such as IT systems, applications, networks, devices, etc.
The primary factor that should guide the mitigation of technology risk is the organizational risk appetite. This means that the organization defines and communicates the amount and type of risk that it is willing to accept or pursue in order to achieve its objectives and strategy.
The organizational risk appetite helps to determine the risk tolerance and thresholds for different risk categories and scenarios, prioritize the risks, select the most suitable risk responses, allocate the resources and budget for risk management, and monitor and report the risk performance and outcomes.
The other options are not the primary factors that should guide the mitigation of technology risk. They are either secondary or not essential for risk management.
The references for this answer are:
Risk IT Framework, page 25
Information Technology & Security, page 19
Risk Scenarios Starter Pack, page 17

NEW QUESTION: 156
Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?
A. Designing compensating controls
B. Determining if KRIs have been updated recently
C. Assessing the effectiveness of the incident response plan
D. Determining what has changed in the environment
Answer: (SHOW ANSWER)
The primary focus of management when key risk indicators (KRIs) begin to rapidly approach defined thresholds is to determine what has changed in the environment. KRIs are metrics that provide information and insight on the current level and trend of the risk exposure, and help to monitor and report the risk status and performance. Defined thresholds are the values or ranges of the KRIs that indicate the acceptable or unacceptable level of the risk exposure, and trigger the risk response actions. When KRIs begin to rapidly approach defined thresholds, it means that the risk exposure is increasing or decreasing significantly, and that the risk situation and status may have changed. Therefore, the primary focus of management is to determine what has changed in the environment, which is the internal or external context that influences or affects the risk exposure and impact. Determining what has changed in the environment helps to identify and analyze the causes, drivers, or factors of the risk change, and to evaluate the implications and consequences of the risk change. Determining what has changed in the environment also helps to update and adjust the risk assessment and response, and to communicate and escalate the risk change to the relevant

stakeholders. Designing compensating controls, determining if KRIs have been updated recently, and assessing the effectiveness of the incident response plan are not the primary focus of management, as they are either the outputs or the inputs of the risk change analysis, and they do not address the primary need of understanding the risk change. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 50.

NEW QUESTION: 157
Which of the following is the PRIMARY benefit of integrating risk and security requirements in an organization's enterprise architecture (EA)?
A. Adherence to legal and compliance requirements
B. Reduction in the number of test cases in the acceptance phase
C. Establishment of digital forensic architectures
D. Consistent management of information assets
Answer: D (LEAVE A REPLY)
Integrating risk and security requirements in an organization's enterprise architecture (EA) helps to ensure that information assets are consistently managed throughout their life cycle, and that the risks associated with them are identified and mitigated. (Risk and Information Systems Control Review Questions, Answers & Explanations Manual, 5th Edition, page 112)

NEW QUESTION: 158
Which of the following is the BEST metric to measure employee adherence to organizational security policies?
A. Total number of security policy audit findings
B. Total number of regulatory violations
C. Total number of security policy exceptions
D. Total number of opened phishing emails
Answer: (SHOW ANSWER)
Tracking opened phishing emails provides a real-time behavioral indicator of how well employees follow security awareness and email policies. It is a leading metric of adherence and risk awareness.
Reference:CRISC Manual - Domain 4, Slide 420-422

NEW QUESTION: 159
Which of the following is the PRIMARY reason to aggregate risk assessment results from different business units?
A. To improve communication of risk to senior management
B. To compare risk profiles across the business units
C. To allocate budget for risk management resources
D. To determine overall impact to the organization
Answer: (SHOW ANSWER)
Aggregating risk assessment results helps evaluate the total exposure and provides a consolidated view of risk, supporting enterprise-wide decision-making.
Reference:CRISC Manual - Domain 2, Slide 191

NEW QUESTION: 160

The BEST criteria when selecting a risk response is the:

A. capability to implement the response

B. importance of IT risk within the enterprise

C. effectiveness of risk response options

D. alignment of response to industry standards

Answer: (SHOW ANSWER)

The effectiveness of risk response options is the best criteria when selecting a risk response, because it reflects the degree to which the response can reduce the impact or likelihood of the risk, or enhance the benefit or opportunity of the risk. The effectiveness of risk response options can be evaluated by considering factors such as cost, feasibility, timeliness, and alignment with the organization's objectives and risk appetite. The other options are not as good as the effectiveness of risk response options, because they do not measure the outcome or value of the response, but rather focus on the input or process of the response, as explained below:

A). Capability to implement the response is a criteria that considers the availability and adequacy of the resources, skills, and knowledge required to execute the response. While this is an important factor to consider, it does not indicate how well the response can address the risk or achieve the desired result.

B). Importance of IT risk within the enterprise is a criteria that considers the significance and priority of the risk in relation to the organization's strategy, objectives, and operations. Whilethis is an important factor to consider, it does not indicate how well the response can address the risk or achieve the desired result.

D). Alignment of response to industry standards is a criteria that considers the compliance and conformity of the response with the best practices, norms, and expectations of the industry or sector. While this is an important factor to consider, it does not indicate how well the response can address the risk or achieve the desired result. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.2, page 40. How to Select Your Risk Responses -Rebel's Guide to Project Management, Risk Response Plan in Project Management: Key Strategies & Tips, Risk Responses - options for managing risk - Stakeholdermap.

com

NEW QUESTION: 161

Avoiding a business activity removes the need to determine:

A. systemic risk

B. residual risk

C. inherent risk

D. control risk

Answer: (SHOW ANSWER)

Avoidancemeans the risk is no longer relevant because the activity is not pursued. As a result, there isno residual riskto manage or control. ISACA's risk response options include avoidance, which eliminates the need for further risk treatment.

NEW QUESTION: 162
Which of the following should be the risk practitioner s FIRST course of action when an organization has decided to expand into new product areas?
A. Identify any new business objectives with stakeholders.
B. Present a business case for new controls to stakeholders.
C. Revise the organization's risk and control policy.
D. Review existing risk scenarios with stakeholders.
Answer: (SHOW ANSWER)
The first course of action for the risk practitioner when an organization has decided to expand into new product areas is to identify any new business objectives with stakeholders. Business objectives are the specific, measurable, achievable, relevant, and time-bound (SMART) goals that the organization aims to accomplish through its products and services. Stakeholders are the parties who have an interest or influence in the organization and its products and services, such as customers, employees, shareholders, suppliers, regulators, or competitors. Identifying any new business objectives with stakeholders is the first course of action, because it helps to understand and define the purpose, scope, and criteria of the new product areas, and to align them with the organization's vision, mission, and strategy. Identifying any new business objectives with stakeholders also helps to establish the expectations, needs, and requirements of the stakeholders, and to ensure their engagement and support for the new product areas. Identifying any new business objectives with stakeholders is the basis for the subsequent risk management activities, such as identifying, analyzing, evaluating, and responding to the risks associated with the new product areas. The other options are not the first course of action, although they may be related or subsequent steps in the risk management process.
Presenting a business case for new controls to stakeholders is a part of the risk response process, which involves selecting and executing the appropriate actions to reduce, avoid, share, or exploit the risks associated with the new product areas. Presenting a business case for new controls to stakeholders can help to justify and communicate the value and impact of the new controls, and to obtain the approval and resources for implementing them. However, this is not the first course of action, as it depends on the identification and prioritization of the business objectives and the risks. Revising the organization's risk and control policy is a part of the risk governance process, which involves defining and updating the rules and guidelines for managing the risks and the controls associated with the new product areas. Revising the organization's risk and control policy can help to ensure the consistency and effectiveness of the risk management process, and to comply with the relevant laws and regulations. However, this is not the first course of action, as it follows the identification and assessment of the business objectives and the risks.
Reviewing existing risk scenarios with stakeholders is a part of the risk monitoring and review process, which involves evaluating and improving the performance and outcomes of the risk management process for the new product areas. Reviewing existing risk scenarios with stakeholders can help to identify and address any changes or issues in the risk levels or the risk responses, and to provide feedback and learning for the risk management process. However, this is not the first course of action, as it requires the identification and analysis of the business objectives and the risks. References = Risk Scenarios Toolkit - ISACA, How to Write Strong Risk Scenarios and Statements - ISACA, The Role of Executive Management in ERM - Corporate Compliance Insights

NEW QUESTION: 163
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?
A. Percentage of vulnerabilities remediated within the agreed service level
B. Number of vulnerabilities identified during the period
C. Number of vulnerabilities re-opened during the period
D. Percentage of vulnerabilities escalated to senior management
Answer: (SHOW ANSWER)
A vulnerability management process is a process that identifies, analyzes, prioritizes, and remediates the vulnerabilities in the IT systems and applications. The effectiveness of a vulnerability management process can be measured by the key performance indicators (KPIs) that reflect the achievement of the process objectives and the alignment with the enterprise's risk appetite and tolerance. The best KPI to measure the effectiveness of a vulnerability management process is the percentage of vulnerabilities remediated within the agreed service level. This KPI indicates how well the process is able to address the vulnerabilities in a timely and efficient manner, and reduce the exposure and impact of the risks associated with the vulnerabilities. The other options are not as good as the percentage of vulnerabilities remediated within the agreed service level, as they may not reflect the quality or timeliness of the remediation actions, or the alignment with the enterprise's risk appetite and tolerance. References = Risk and Information Systems Control Study Manual,
7th Edition, Chapter 4, Section 4.3.2.1, pp. 171-172.

NEW QUESTION: 164
Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?
A. KCIs are independent from KRIs KRIs.
B. KCIs and KRIs help in determining risk appetite.
C. KCIs are defined using data from KRIs.
D. KCIs provide input for KRIs
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics that provide information on the level of exposure to a given risk. Key control indicators (KCIs) are metrics that measure the performance or effectiveness of a control in mitigating a risk. KCIs provide input for KRIs, because they help to assess the residual risk after applying the control. For example, if the KRI is the number of security incidents, and the KCI is the percentage of incidents detected by the intrusion prevention system (IPS), then the KCI provides input for the KRI by showing how well the IPS is reducing the risk of security breaches. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 165
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

A. Qualitative measures require less ongoing monitoring.
B. Qualitative measures are better aligned to regulatory requirements.
C. Qualitative measures are better able to incorporate expert judgment.
D. Qualitative measures are easier to update.
Answer: (SHOW ANSWER)
Qualitative measures are methods of expressing risk levels using descriptive terms, such as high, medium, or low, based on subjective criteria, such as likelihood, impact, or severity. Qualitative measures are often used to identify and prioritize risks, and to communicate risk information to stakeholders1.
Residual risk is the level of risk that remains after the risk response has been implemented. Residual risk reflects the effectiveness and efficiency of the risk response, and the need for further action or monitoring2.
Emerging threats are new or evolving sources or causes of risk that have the potential to adversely affect the organization's objectives, assets, or operations. Emerging threats are oftencharacterized by uncertainty, complexity, and ambiguity, and may require innovative or adaptive risk responses3.
The best reason to use qualitative measures to express residual risk levels related to emerging threats is that qualitative measures are better able to incorporate expert judgment. Expert judgment is the opinion or advice of a person or a group of people who have specialized knowledge, skills, or experience in a particular domain or field. Expert judgment can help to:
Provide insights and perspectives on the nature and characteristics of the emerging threats, and their possible causes and consequences Assess the likelihood and impact of the emerging threats, and their interactions and dependencies with other risks Evaluate the suitability and effectiveness of the risk responses, and their alignment with the organization's risk appetite and tolerance Identify and recommend the best practices and lessons learned for managing the emerging threats, and for improving the risk management process45 Qualitative measures are better able to incorporate expert judgment than quantitative measures, which are methods of expressing risk levels using numerical or measurable values, such as percentages, probabilities, or monetary amounts. Quantitative measures are often used to estimate and analyze risks, and to support risk decision making1. However, quantitative measures may not be suitable or feasible for expressing residual risk levels related to emerging threats, because:
Quantitative measures require reliable and sufficient data and information, which may not be available or accessible for the emerging threats Quantitative measures rely on mathematical models and techniques, which may not be able to capture or reflect the complexity and uncertainty of the emerging threats Quantitative measures may create a false sense of precision or accuracy, which may not be justified or warranted for the emerging threats Quantitative measures may be influenced or manipulated by biases or assumptions, which may not be valid or appropriate for the emerging threats67 Therefore, qualitative measures are better able to incorporate expert judgment, which can enhance the understanding and management of the residual risk levels related to emerging threats.
The other options are not the best reasons to use qualitative measures to express residual risk levels related to emerging threats, but rather some of the advantages or disadvantages of qualitative measures. Qualitative measures require less ongoing monitoring than quantitative measures, because they are simpler and easier to apply and update. However, this does not mean that qualitative measures can eliminate or reduce the need for monitoring, which is an essential part of the risk management process. Qualitative measures are better aligned to regulatory requirements than quantitative measures, because they are more consistent and

comparable across different domains and contexts. However, this does not mean that qualitative measures can satisfy or comply with all the regulatory requirements, which may vary depending on theindustry or sector. Qualitative measures are easier to update than quantitative measures, because they do not depend on complex calculations or formulas. However, this does not mean that qualitative measures can always reflect the current or accurate risk levels, which may change over time or due to external factors. References = Qualitative Risk Analysis vs. Quantitative Risk Analysis - ISACA Residual Risk - ISACA Emerging Threats - ISACA Expert Judgment - ISACA Expert Judgment in Project Management: Narrowing the Theory-Practice Gap Quantitative Risk Analysis - ISACA Quantitative Risk Analysis: A Critical Review
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 166
In the three lines of defense model, a PRIMARY objective of the second line is to:
A. Review and evaluate the risk management program.
B. Ensure risks and controls are effectively managed.
C. Implement risk management policies regarding roles and responsibilities.
D. Act as the owner for any operational risk identified as part of the risk program.
Answer: (SHOW ANSWER)
The second line of defense provides oversight to ensure risks and controls are effectively managed. This includes compliance, risk management policies, and performance monitoring, aligning withRisk Governanceframeworks and enhancing the organization's risk resilience.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167
The PRIMARY reason for communicating risk assessment results to data owners is to enable the:
A. design of appropriate controls.
B. industry benchmarking of controls.
C. prioritization of response efforts.
D. classification of information assets.
Answer: (SHOW ANSWER)
Understanding the Question:
The question focuses on the primary reason for communicating risk assessment results to data owners.
Analyzing the Options:
A: Design of appropriate controls:This is important but not the primary reason for communication.
B: Industry benchmarking of controls:This is secondary to the main goal of communicating risk.

C: Prioritization of response efforts:This enables data owners to allocate resources and address the most critical risks first.
D: Classification of information assets:This is typically part of the initial risk assessment process, not the main communication goal.
Communication of Risk Assessment Results:Ensuring data owners understand the results of risk assessments allows them to make informed decisions on where to focus their efforts.
Prioritization:Data owners can prioritize their actions based on the assessed risk levels, ensuring that resources are allocated efficiently to mitigate the most significant risks.
References:
CRISC Review Manual, Chapter 3: Risk Response and Reporting, details the importance of communicating risk assessment results for effective risk management and response prioritization.

NEW QUESTION: 168
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?
A. Acquisition
B. Implementation
C. Initiation
D. Operation and maintenance
Answer: (SHOW ANSWER)
The acquisition phase of the system development life cycle (SDLC) is the phase where the organization decides to purchase a new IT system from an external vendor or develop it internally. During this phase, the identified risks will most likely lead to architecture and design trade-offs, as the organization will have to balance the cost, quality, functionality, security, and performance of the new IT system. The organization will have to evaluate the different options and alternatives available, and select the one that best meets the business needs and the risk appetite. The other phases of the SDLC are not as likely to involve architecture and design trade-offs, as they are more focused on implementing, testing, deploying, and maintaining the new IT system. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.2: IT Risk Response Options, page 133.

NEW QUESTION: 169
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?
A. IT infrastructure head
B. Human resources head
C. Supplier management head
D. Application development head
Answer: (SHOW ANSWER)
Data confidentiality risk is the risk that the data may be accessed, disclosed, or modified by unauthorized parties, resulting in breaches of privacy, trust, or compliance1. Platform as a Service (PaaS) is a cloud computing model that provides a platform for developing, testing, and deploying applications, without

requiring the users to manage the underlying infrastructure2. An internally developed payroll application is an application that is created and maintained by the organization itself, rather than by a third-party vendor, and that is used to process and manage the payroll data of the organization's employees3. The owner of the data confidentiality risk is the person or entity that has the authority and accountability for the data and its protection, and that is responsible for identifying, assessing, and mitigating the risk. The owner of the data confidentiality risk related to an internally developed payroll application that leverages PaaS infrastructure from the cloud is the human resources head, as they are the person who oversees the human resources function and the payroll data of the organization. The human resources head has the best understanding of the sensitivity, value, and usage of the payroll data, and the potential impacts and implications of a data confidentiality breach. The human resources head also has the ability and responsibility to define and implement the policies, procedures, and controls that are necessary to protect the payroll data, and to monitor and report on the performance and compliance of the data confidentiality risk management. The IT infrastructure head, the supplier management head, and the application development head are not the best choices for owning the data confidentiality risk related to an internally developed payrollapplication that leverages PaaS infrastructure from the cloud, as they do not have the same level of authority and accountability as the human resources head. The IT infrastructure head is the person who oversees the IT infrastructure function and the PaaS infrastructure of the organization. The IT infrastructure head may be involved in providing input and feedback to the human resources head on the data confidentiality risk management, especially those related to the PaaS infrastructure, but they do not have the final say or the overall responsibility for the payroll data and its protection. The supplier management head is the person who oversees the supplier management function and the relationship with the cloud service provider that provides the PaaS infrastructure. The supplier management head may be involved in negotiating and enforcing the service level agreements and the security requirements with the cloud service provider, but they do not have the authority or the expertise to manage the data confidentiality risk of the payroll data. The application development head is the person who oversees the application development function and the development, testing, and deployment of the payroll application. The application development head may be involved in designing and implementing the security features and controls of the payroll application, but they do not have the perspective or the influence to manage the data confidentiality risk of the payroll data. References = 3: Payroll Software: What Is It & How Does It Work? | QuickBooks2: What is Platform as a Service (PaaS)? | IBM1: Data Confidentiality: Identifyingand Protecting Assets Against Data ... : [Risk Ownership - Risk Management] : [Human Resources and Payroll Security Policy - University of ...] : [Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.1: IT Risk Concepts, pp. 17-19.] : [Risk andInformation Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.1: Risk Identification, pp. 57-59.] : [Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.1: Control Design, pp. 233-235.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.2: Control Implementation, pp. 243-245.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.3: Control Monitoring and Maintenance, pp. 251-253.]

NEW QUESTION: 170

Which of the following problems is BEST solved by a cloud access security broker (CASB)?

A. Lack of expertise to implement single sign-on (SSO)

B. Cloud access security vendor selection

C. Inadequate key management policies

D. Inconsistently applied security policies

Answer: (SHOW ANSWER)

A Cloud Access Security Broker (CASB) acts as a control point between cloud service users and providers to enforce the organization's security policies consistently across all cloud applications.

CRISC-aligned cloud risk guidance explains:

"CASBs provide visibility, data security, threat protection, and compliance enforcement by applying consistent security controls across all cloud services." Therefore, the main issue CASBs address is inconsistent security policy enforcement between on-premise and multiple cloud environments.

Option details:

* A and C (SSO and key management) relate to identity or encryption control tools.

* B is unrelated to CASB's purpose.

Hence, D. Inconsistently applied security policies is correct.

CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Cloud Risk Controls.

NEW QUESTION: 171

Which of the following is MOST effective in continuous risk management process improvement?

A. Periodic assessments

B. Change management

C. Awareness training

D. Policy updates

Answer: (SHOW ANSWER)

Continuous risk management process improvement is the practice of evaluating and enhancing the risk management process on a regular basis, to ensure that it is effective, efficient, and aligned with the business objectives and strategy. Continuous risk management processimprovement can help identify and address the gaps, weaknesses, or opportunities for improvement in the risk management process, and ensure that the process is responsive and adaptable to the changing risk environment. The most effective method for continuous risk management process improvement is periodic assessments, which are systematic and objective evaluations of the risk management process, performed at predefined intervals or after significant events. Periodic assessments can help measure and monitor the performance and maturity of the risk management process, using criteria such as the risk management framework, standards, policies, procedures, methods, tools, roles, responsibilities, and results. Periodic assessments can also help identify and analyze the strengths, weaknesses, threats, and opportunities of the risk management process, and provide feedback and recommendations for improvement. Periodic assessments can also help communicate and report the status and progress of the risk management process to the stakeholders, and obtain their

input and support for improvement actions. References = Continuous Risk Management Guidebook, p. 7-8, ISO 31000:
riskmanagement and its continuous improvement, How Continuous Monitoring Drives Risk Management.

NEW QUESTION: 172
An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?
A. Periodically review application on BYOD devices
B. Include BYOD in organizational awareness programs
C. Implement BYOD mobile device management (MDM) controls.
D. Enable a remote wee capability for BYOD devices
Answer: C (LEAVE A REPLY)
The best way to mitigate the security risk associated with the inappropriate use of enterprise applications on the BYOD devices is to implement BYOD mobile device management (MDM) controls. MDM controls are software tools or services that allow the organization to remotely manage, monitor, and secure the BYOD devices and the enterprise applications and data on them. MDM controls can help to enforce security policies, restrict unauthorized access, encrypt sensitive data, wipe data in case of loss or theft, and update or patch applications. The other options are not as effective as implementing MDM controls, as they are related to the review, awareness, or recovery of the BYOD devices and applications, not the prevention or protection of the security risk. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 173
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?
A. Risk and control ownership
B. Senior management participation
C. Business unit support
D. Risk nomenclature and taxonomy
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, risk nomenclature and taxonomy is the set of terms and definitions that are used to describe and classify risks and their attributes. Risk nomenclature and taxonomy is the most important consideration when aligning IT risk management with the enterprise risk management (ERM) framework, as it helps to ensure a common and consistent understanding and communication of risks across the organization. Risk nomenclature and taxonomy also helps to integrate and harmonize the IT risk management processes and activities with the ERM framework, and to facilitate the aggregation and reporting of risks at different levels of the organization. References = CRISC Review Manual1, page 197.

NEW QUESTION: 174
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

A. Classification of the data
B. Type of device
C. Remote management capabilities
D. Volume of data
Answer: (SHOW ANSWER)
The most important factor when assessing the risk of allowing users to access company data from their personal devices is the classification of the data, as it indicates the level of sensitivity, confidentiality, and criticality of the data. Data classification helps to determine the appropriate level of protection and controls that are needed to prevent unauthorized access, disclosure, modification, or loss of the data. Data classification also helps to define the roles and responsibilities of the data owners, custodians, and users, and the acceptable use of the data. The other options are not the most important factors, although they may be relevant or influential in the risk assessment. The type of device may affect the security features and vulnerabilities of the device, but it does not determine the value or impact of the data. The remote management capabilities may affect the ability to monitor, control, or wipe the device in case of theft or loss, but they do not reflect the nature or purpose of the data. The volume of data may affect the storage capacity or performance of the device, but it does not indicate the importance or significance of the data. References = What is BYOD (Bring-Your-Own-Device) - CrowdStrike; Understanding BYOD Policy - Get Certified Get Ahead; Addressing cyber security concerns on employees' personal devices; Personal Devices at Work - Nonprofit Risk Management Center; 10 Keys to an Effective BYOD and Remote Access Policy

NEW QUESTION: 175
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?
A. KRI design must precede definition of KCIs.
B. KCIs and KRIs are independent indicators and do not impact each other.
C. A decreasing trend of KRI readings will lead to changes to KCIs.
D. Both KRIs and KCIs provide insight to potential changes in the level of risk.
Answer: (SHOW ANSWER)
KRIs and KCIs are both metrics that measure and monitor the risk and control environment of an enterprise. KRIs are indicators that reflect the level and trend of risk exposure, and help to identify potential risk events or issues. KCIs are indicators that reflect the performance and effectiveness of the risk controls, and help to ensure that the controls are operating as intended and mitigating the risk. Both KRIs and KCIs provide insight to potential changes in the level of risk, as they can signal the need for risk response actions, such as enhancing, modifying, or implementing new controls, or adjusting the risk strategy and objectives. References = Most Asked CRISC Exam Questions and Answers. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 240.

NEW QUESTION: 176
Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?
A. Qualitative measures for potential loss events

B. Changes in owners for identified IT risk scenarios
C. Changes in methods used to calculate probability
D. Frequent use of risk acceptance as a treatment option
Answer: (SHOW ANSWER)
Changes in methods used to calculate probability present the greatest challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels, as they may introduce inconsistency and incomparability in the risk assessment results over time. Probability is a key factor in determining the level and priority of IT risks, and different methods may produce different values for the same risk scenario. For example, some methods may use historical data, expert judgment, or simulation techniques to estimate the likelihood of a risk event. If the methods used to calculate probability change frequently or vary across different business units or processes, the IT risk practitioner may face difficulty in aggregating, normalizing, and reporting the risk levels and trends. The other options are not the greatest challenges for reporting on trends in historical IT risk levels, although they may pose some difficulties or limitations. Qualitative measures for potential loss events are subjective and imprecise, but they can still provide a relative ranking of risks and their impacts. Changes in owners for identified IT risk scenarios may affect the accountability and responsibility for managing the risks, but they do not necessarily affect the risk levels or trends. Frequent use of risk acceptance as a treatment option may indicate a high risk appetite or tolerance, but it does not prevent the IT risk practitioner from reporting on the risk levels or trends. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk and Control Monitoring and Reporting, page 181.

NEW QUESTION: 177
A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?
A. Implement a tool to create and distribute violation reports
B. Raise awareness of encryption requirements for sensitive data.
C. Block unencrypted outgoing emails which contain sensitive data.
D. Implement a progressive disciplinary process for email violations.
Answer: C (LEAVE A REPLY)
According to the CRISC Review Manual (Digital Version), the most effective approach to mitigate the risk associated with data loss due to users sending sensitive information by email without using encryption is to block unencrypted outgoing emails which contain sensitive data. This is an example of a risk avoidance strategy, which aims to eliminate the risk by removing the source of the risk or the activity that causes the risk. Blocking unencrypted outgoing emails which contain sensitive data can prevent unauthorized access, disclosure, modification or destruction of the sensitive information, and thus protect the confidentiality, integrity and availability of the data. This approach can also deter users from violating the encryption policy and enforce compliance with the security standards and regulations.
References = CRISC Review Manual (Digital Version), Chapter 3: IT Risk Response, Section 3.3: Risk Response Options, pp. 167-1681

NEW QUESTION: 178

What is the MAIN benefit of using a top-down approach to develop risk scenarios?
A. It describes risk events specific to technology used by the enterprise.
B. It establishes the relationship between risk events and organizational objectives.
C. It uses hypothetical and generic risk events specific to the enterprise.
D. It helps management and the risk practitioner to refine risk scenarios.
Answer: (SHOW ANSWER)
The main benefit of using a top-down approach to develop risk scenarios is that it establishes the relationship between risk events and organizational objectives. A top-down approach is a method of risk identification and analysis that starts with the organization's strategic objectives and then identifies the potential risk events that could affect or prevent the achievement of those objectives. A top-down approach helps to establish the relationship between risk events and organizational objectives, because it links the risk scenarios to the organization's mission, vision, values, and strategy, and it prioritizes the risk scenarios based on their impact and relevance to the organization's objectives. A top-down approach also helps to align and communicate the risk scenarios with the organization's stakeholders, such as the board, management, and business units, and to facilitate the risk response and monitoring activities. The other options are not the main benefit of using a top-down approach, although they may be part of or derived from the top-down approach. Describing risk events specific to technology used by the enterprise, using hypothetical and generic risk events specific to the enterprise, and helping management and the risk practitioner to refine risk scenarios are all activities or outcomes that could be performed or achieved by using a top-down approach, but they are not the primary purpose or result of the top-down approach. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 179
Which of the following is the BEST indication that an organization's risk management program has not reached the desired maturity level?
A. Significant increases in risk mitigation budgets
B. Large fluctuations in risk ratings between assessments
C. A steady increase in the time to recover from incidents
D. A large number of control exceptions
Answer: (SHOW ANSWER)
A risk management program is a set of processes, policies, and tools that enable an enterprise to identify, analyze, evaluate, treat, monitor, and communicate its risks. The maturity level of a risk management program indicates how well the program is integrated, standardized, and aligned with the enterprise's objectives, culture, and values. The best indication that an organization's risk management program has not reached the desired maturity level is large fluctuations in risk ratings between assessments. Risk ratings are the measures of the impact and likelihood of the risks, and they should be consistent and comparable across the enterprise and over time. Large fluctuations in risk ratings between assessments suggest that the risk management program is not stable, reliable, or effective, and that the risk identification and analysis methods are not robust, accurate, or transparent. The other options are not as indicative of the maturity level of the risk management program, as they involve different aspects or outcomes of the risk management program:

* Significant increases in risk mitigation budgets means that the enterprise is spending more resources on implementing risk responses, such as controls, policies, or procedures. This may indicate that the enterprise is facing more or higher risks, or that the risk responses are more costly or complex, but it does not necessarily reflect the maturity level of the risk management program, as it may also depend on the enterprise's risk appetite, tolerance, and strategy.
* A steady increase in the time to recover from incidents means that the enterprise is taking longer to restore its normal operations after a disruption or a loss. This may indicate that the enterprise is not prepared or resilient enough to deal with the incidents, or that the incidents are more frequent or severe, but it does not necessarily reflect the maturity level of the risk management program, as it may also depend on the nature and source of the incidents, or the availability and effectiveness of the recovery plans.
* A large number of control exceptions means that the enterprise is deviating from the established controls, policies, or procedures, either intentionally or unintentionally. This may indicate that the enterprise is not complying with the risk management program, or that the controls are not adequate or appropriate for the enterprise's needs, but it does not necessarily reflect the maturity level of the risk management program, as it may also depend on the reasons and justifications for the exceptions, or the approval and monitoring processes for the exceptions. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.1.3.1, pp. 14-15.

NEW QUESTION: 180

When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

Freecram.net

A. Users may share accounts with business system analyst
B. Application may not capture a complete audit trail.
C. Users may be able to circumvent application controls.
D. Multiple connects to the database are used and slow the process
Answer: C (LEAVE A REPLY)
The risk of users circumventing application controls is the most significant exposure when an application uses individual user accounts to access the underlying database. This is because users may have direct access to the data and bypass the validation, authorization, and logging mechanisms that are implemented at the application level. Users may also be able to modify or delete data without proper authorization or audit trail.
The other options are less significant exposures, as they do not directly affect the integrity or confidentiality of the data. References = Risk IT Framework, ISACA, 2009, page 35; CRISC Review Manual, 6th Edition, ISACA, 2015, page 214.

NEW QUESTION: 181
Which of the following would have the GREATEST impact on reducing the risk associated with the implementation of a big data project?
A. Data processing
B. Data quality
C. Data scalability

D. Data governance

Answer: (SHOW ANSWER)

Data governanceprovides a structured framework for handling data access, classification, compliance, and security. It ensures accountability, roles, and control mechanisms-critical formanaging risk in big data environments.

Reference:CRISC Manual - Domain 3, Slide 310-311

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182

Which of the following would be a risk practitioner's GREATEST concern related to the monitoring of key risk indicators (KRIs)?

A. Logs are retained for longer than required.

B. Logs are reviewed annually.

C. Logs are stored in a multi-tenant cloud environment.

D. Logs are modified before analysis is conducted.

Answer: (SHOW ANSWER)

Modifying logs before analysis compromises the integrity and reliability of monitoring processes. This action creates a risk of inaccurate data feeding into key risk indicators, which undermines the effectiveness of monitoring and decision-making. Maintaining log integrity is a foundational practice in Risk Monitoring and Reporting.

NEW QUESTION: 183

An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

A. Conduct a risk assessment.

B. Update the security strategy.

C. Implement additional controls.

D. Update the risk register.

Answer: (SHOW ANSWER)

The FIRST thing that the organization should do to reduce the risk of data exposure when modifying its system to enable acceptance of credit card payments is to conduct a risk assessment, because it is a process that involves identifying and analyzing the potential risks, threats, and vulnerabilities that may affect the system and the data, and their likelihood and impact on the business objectives and processes. A risk assessment can help to determine the current risk level and exposure, and to provide the basis for selecting

and implementing the appropriate risk responses and controls. The other options are not the first thing that the organization should do, because:
* Option B: Updating the security strategy is a result of conducting a risk assessment, but not the first thing that the organization should do. A security strategy is a plan that defines the security objectives, policies, standards, and procedures for the system and the data, and it should be aligned with the risk assessment results and the business requirements and expectations.
* Option C: Implementing additional controls is a response to the risk assessment results, but not the first thing that the organization should do. Controls are the measures that are designed and implemented to prevent or reduce the occurrence or impact of the risks, threats, and vulnerabilities, and to ensure the confidentiality, integrity, and availability of the system and the data.
* Option D: Updating the risk register is a part of the risk assessment process, but not the first thing that the organization should do. A risk register is a tool that documents and tracks the identified risks, their characteristics, their status, and their responses, and it should be updated regularly to reflect the current risk profile and exposure of the system and the data. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 108.

NEW QUESTION: 184
Which of the following BEST enables a risk practitioner to identify the consequences of losing critical resources due to a disaster?
A. Risk management action plans
B. Business impact analysis (BIA)
C. What-if technique
D. Tabletop exercise results
Answer: (SHOW ANSWER)
Business Impact Analysis (BIA):
Purpose: A BIA is a systematic process to evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.
Identification of Consequences: It identifies critical resources and the consequences of their loss, allowing an organization to determine the operational and financial impacts of such losses.
Steps Involved in BIA:
Identify Critical Functions: Determine which business functions and processes are essential to the organization's operations.
Assess Impact: Evaluate the impact of losing these functions on the organization's ability to operate.
Estimate Downtime Tolerance: Determine the maximum allowable downtime for critical functions before significant harm occurs.
Identify Dependencies: Document dependencies between systems, processes, and resources to understand how disruptions to one part affect the whole.
Comparison with Other Options:
Risk Management Action Plans: These are detailed plans developed to address identified risks but do not specifically focus on the impact of losing critical resources.

What-if Technique: This is a brainstorming technique used to explore potential risks and their impacts but is not as structured as a BIA.
Tabletop Exercise Results: These exercises simulate disaster scenarios to test response plans but do not provide the comprehensive impact analysis that a BIA does.
Best Practices:
Regular Updates: Regularly update the BIA to reflect changes in the business environment and operational dependencies.
Integration with DR/BC Plans: Ensure that findings from the BIA are integrated into disaster recovery (DR) and business continuity (BC) plans to enhance overall preparedness.
References:
CRISC Review Manual: Discusses the importance of BIA in identifying the impacts of losing critical resources and guiding the development of effective risk management strategies.
ISACA Standards: Highlight the role of BIA in evaluating the consequences of resource loss and informing business continuity planning.

NEW QUESTION: 185
Which of the following is the BEST response when a potential IT control deficiency has been identified?
A. Remediate and report the deficiency to the enterprise risk committee.
B. Verify the deficiency and then notify the business process owner.
C. Verify the deficiency and then notify internal audit.
D. Remediate and report the deficiency to senior executive management.
Answer: (SHOW ANSWER)
Verifying the deficiency and then notifying the business process owner is the best response when a potential IT control deficiency has been identified. This is because verifying the deficiency can help confirm the existence, nature, and extent of the deficiency, as well as its root causes and impacts. Notifying the business process owner can help ensure that the deficiency is communicated to the person who is responsible for the process and its outcomes, and who has the authority and accountability to take appropriate actions to address the deficiency. According to the CRISC Review Manual 2022, one of the key risk response techniques is to report the risk to the relevant stakeholders, such as the business process owners1.
According to the CRISC Review Questions, Answers & Explanations Manual 2022, verifying the deficiency and then notifying the business process owner is the correct answer to this question2.
Remediating and reporting the deficiency to the enterprise risk committee or senior executive management are not the best responses when a potential IT control deficiency has been identified. These are possible actions that can be taken after the deficiency has been verified and notified to the business process owner, but they are not the first or immediate responses. Remediating the deficiency without verifying it can lead to ineffective or inappropriate solutions, as well as wasted time and resources. Reporting the deficiency to the enterprise risk committee or senior executive management without notifying the business process owner can create confusion, conflict, or delay in the risk response process, as well as undermine the ownership and accountability of the business process owner.

NEW QUESTION: 186

Which of the following BEST enables a risk practitioner to focus on risk factors that could potentially affect the results of an IT initiative?

A. Prioritizing threats and controls

B. Assessing trends in quantitative risk analysis results

C. Measuring and reporting qualitative risk trends

D. Conducting stakeholder surveys

Answer: (SHOW ANSWER)

Prioritizing threats and controls helps tofocus resources and mitigationon high-risk elements that directly impact project objectives. This enhances decision-making and project alignment with business goals.

Reference:CRISC Manual - Domain 2, Slide 170-173

NEW QUESTION: 187

Which of the following is MOST important for a risk practitioner to consider when analyzing the risk associated with migrating to a new cloud service provider?

A. Past incidents related to acquired cloud services

B. The cloud service provider's control environment

C. The complexity of the cloud services

D. The date of the cloud service provider's last risk assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 188

The BEST use of key risk indicators (KRIs) is to provide:

A. Early indication of increasing exposure to a specific risk.

B. Lagging indication of major information security incidents.

C. Early indication of changes to required risk response.

D. Insight into the performance of a monitored process.

Answer: (SHOW ANSWER)

Key risk indicators are designed to provide early warnings about increasing risk exposure, enabling timely risk mitigation efforts. This supports proactive risk management, as outlined in the Risk Monitoring and Reporting domain of CRISC.

NEW QUESTION: 189

An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

A. The third party's IT operations manager

B. The organization's process owner

C. The third party's chief risk officer (CRO)

D. The organization's risk practitioner

Answer: B (LEAVE A REPLY)

The organization's process owner should own the risk of exposing the payroll data due to a control weakness at the third party, because the process owner is the person who is responsible for the business process that

generates, uses, or transfers the payroll data. The process owner should also ensure that the third party complies with the contractual obligations and service level agreements that define the expected performance and security standards of the payroll data processing. The other options are not the correct answers, because they are not the primary owners of the risk, although they may also be involved in the risk management process. The third party's IT operations manager, the third party's chief risk officer (CRO), and the organization's risk practitioner are examples of secondary owners or stakeholders of the risk, who may provide support, guidance, or oversight to the risk owner, but they are not accountable for the risk or the risk response strategy. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 190

An organization's senior management is considering whether to acquire cyber insurance. Which of the following is the BEST way for the risk practitioner to enable management's decision?

Freecram.net

A. Perform a cost-benefit analysis.
B. Conduct a SWOT analysis.
C. Provide data on the number of risk events from the last year.
D. Report on recent losses experienced by industry peers.
Answer: (SHOW ANSWER)
Acost-benefit analysisevaluates the financial implications of acquiring cyber insurance versus the potential loss exposure. This approach enables informed decision-making by comparing the insurance cost with the potential savings from covered risks.

NEW QUESTION: 191
Which of the following is the BEST way to determine the ongoing efficiency of control processes?
A. Perform annual risk assessments.
B. Interview process owners.
C. Review the risk register.
D. Analyze key performance indicators (KPIs).
Answer: (SHOW ANSWER)
* Control processes are the procedures and activities that aim to ensure the effectiveness and efficiency of the organization's operations, the reliability of its information, and the compliance with its policies and regulations12.
* The ongoing efficiency of control processes is the degree to which the control processes achieve their intended results with minimum resources, costs, or waste34.
* The best way to determine the ongoing efficiency of control processes is to analyze key performance indicators (KPIs), which are quantifiable measures of progress toward an intended result, such as a strategic objective or a desired outcome56.
* Analyzing KPIs is the best way because it provides a systematic and consistent method of evaluating the performance of the control processes, and identifying the areas of improvement or optimization56.
* Analyzing KPIs is also the best way because it enables the organization to monitor and report the efficiency of the control processes to the relevant stakeholders, and to take corrective or preventive actions when necessary56.

* The other options are not the best way, but rather possible sources of information or inputs that may support or complement the analysis of KPIs. For example:
* Performing annual risk assessments is a way to identify and evaluate the risks that may affect the organization's objectives, and to determine the adequacy and effectiveness of the control processes in mitigating those risks12. However, this way is not the best because it is periodic rather than continuous, and may not capture the changes or trends in the efficiency of the control processes12.
* Interviewing process owners is a way to collect and verify the information and feedback from the people who are responsible for designing, implementing, and operating the control processes12. However, this way is not the best because it is subjective and qualitative, and may not provide reliable or comparable data on the efficiency of the control processes12.
* Reviewing the risk register is a way to examine and update the documentation and status of the risks and the control processes that are associated with them12. However, this way is not the best because it is descriptive rather than analytical, and may not measure or evaluate the efficiency of the control processes12.
References =
* 1: Risk IT Framework, ISACA, 2009
* 2: IT Risk Management Framework, University of Toronto, 2017
* 3: The Control Process | Principles of Management4
* 4: Control Management: What it is + Why It's Essential | Adobe Workfront5
* 5: What is a Key Performance Indicator (KPI)? Guide & Examples - Qlik1
* 6: What is a Key Performance Indicator (KPI)? - KPI.org2

NEW QUESTION: 192
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?
A. Conducting a business impact analysis (BIA)
B. Identifying the recovery response team
C. Procuring a recovery site
D. Assigning sensitivity levels to data
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, conducting a business impact analysis (BIA) is the task that should be completed prior to creating a disaster recovery plan (DRP), because it helps to identify the critical business processes and resources, and their dependencies, that need to be recovered in the event of a disaster. The BIA also helps to determine the recovery time objectives (RTOs) and recovery point objectives (RPOs) for each business process and resource, which are the key inputs for the DRP. The other options are not the tasks that should be completed prior to creating a DRP, as they are part of the DRP itself. Identifying the recovery response team is the task of defining the roles and responsibilities of the personnel involved in the recovery process. Procuring a recovery site is the task of selecting and acquiring an alternative location where the business operations can be resumed. Assigning sensitivity levels to data is the task of classifying the data based on its importance and protection requirements. References = CRISC Review Manual, 7th Edition, Chapter 5, Section 5.2.1, page 237.

NEW QUESTION: 193

An organization is reviewing a contract for a Software as a Service (SaaS) sales application with a 99.9% uptime service level agreement (SLA). Which of the following BEST describes ownership of availability risk?
A. The risk is shared by both organizations.
B. The liability for the risk is owned by the cloud provider.
C. The risk is transferred to the cloud provider.
D. The liability for the risk is owned by the sales department.
Answer: (SHOW ANSWER)
Even with SLAs in place, both parties must manage aspects of availability risk. The provider manages infrastructure, while the organization is responsible for business impact.
Reference:CRISC Manual - Domain 1: Governance, Slide 41, 268

NEW QUESTION: 194
Which of the following is the BEST way to reduce the likelihood of an individual performing a potentially harmful action as the result of unnecessary entitlement?
A. Application monitoring
B. Separation of duty
C. Least privilege
D. Nonrepudiation
Answer: (SHOW ANSWER)
Least privilege is the best way to reduce the likelihood of an individual performing a potentially harmful action as the result of unnecessary entitlement, because it limits the access and permissions of the individual to the minimum level that is required to perform their role or function, and prevents the individual from accessing or modifying the resources or data that are not relevant or authorized. An entitlement is a right or privilege that grants an individual the ability to access or use a resource or data, such as a file, a system, or an application. An unnecessary entitlement is an entitlement that is not needed or justified for the individual's role or function, and may pose a risk of unauthorized or inappropriate access or use of the resource or data. A potentially harmful action is an action that may cause harm or damage to the organization or its objectives, such as a data breach, a fraud, or a sabotage. Least privilege is the best way, as it helps to minimize the exposure and impact of the unnecessary entitlement, and to reduce the likelihood and severity of the potentially harmful action. Application monitoring, separation of duty, and nonrepudiation are all possible ways to reduce the likelihood of an individual performing a potentially harmful action as the result of unnecessary entitlement, but they are not the best way, as they do not directly address the unnecessary entitlement, and may not prevent the potentially harmful action. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.3.2, page 200

NEW QUESTION: 195
A risk practitioner learns that a risk owner has been accepting gifts from a supplier of IT products. Some of these IT products are used to implement controls and to mitigate risk to acceptable levels. Which of the following should the risk practitioner do FIRST?
A. Initiate disciplinary action against the risk owner.
B. Reassess the risk and review the underlying controls.

C. Review organizational ethics policies.
D. Report the activity to the supervisor.
Answer: (SHOW ANSWER)
Reporting the activity to the supervisor is the first thing that the risk practitioner should do when learning that a risk owner has been accepting gifts from a supplier of IT products. This is because accepting gifts from a supplier of IT products can create a conflict of interest, compromise the integrity and objectivity of the risk owner, and violate the organizational ethics policies. Reporting the activity to the supervisor can help ensure that the issue is escalated to the appropriate authority, investigated, and resolved in a timely and transparent manner. According to the CRISC Review Manual 2022, one of the key risk response techniques is to report the risk to the relevant stakeholders, such as the supervisor1. According to the web search results, reporting the activity to the supervisor is a common and recommended action when encountering a potential ethical violation in the workplace

NEW QUESTION: 196
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?
A. An analysis of the security logs that illustrate the sequence of events
B. An analysis of the impact of similar attacks in other organizations
C. A business case for implementing stronger logical access controls
D. A justification of corrective action taken
Answer: A (LEAVE A REPLY)
An analysis of the security logs that illustrate the sequence of events is the most important information for the person responsible for managing the incident, as it can help to identify the source, scope, and impact of the security breach, and to determine the appropriate response actions. An analysis of the security logs can also provide evidence for forensic investigation and legal action, and help to prevent or mitigate future incidents by identifying the root causes and vulnerabilities. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 235. CRISC by Isaca Actual Free Exam Q&As, Question 9. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 235. CRISC Sample Questions 2024, Question 235.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 197
Which of the following is MOST important for an organization to consider when developing its IT strategy?
A. IT goals and objectives

B. Organizational goals and objectives
C. The organization's risk appetite statement
D. Legal and regulatory requirements
Answer: (SHOW ANSWER)
The most important factor for an organization to consider when developing its IT strategy is the organizational goals and objectives. The organizational goals and objectives are the statements that define the purpose, direction, and desired outcomes of the organization. The organizational goals and objectives help to align the IT strategy with the organization's mission, vision, values, and strategy, and to ensure that the IT strategy supports and enables the organization's performance and improvement. The organizational goals and objectives also help to communicate and coordinate the IT strategy with the organization's stakeholders, such as the board, management, business units, and IT functions, and to facilitate the IT decision-making and reporting processes. The other options are not as important as the organizational goals and objectives, although they may be related to the IT strategy. IT goals and objectives, the organization's risk appetite statement, and legal and regulatory requirements are all factors that could affect the feasibility and sustainability of the IT strategy, but they do not necessarily reflect or influence the organization's purpose, direction, and desired outcomes. References = Risk and Information Systems Control Study Manual, Chapter
1, Section 1.2.1, page 1-9.

NEW QUESTION: 198
Which of the following is a PRIMARY objective of privacy impact assessments (PIAs)?
A. To ensure compliance with data privacy laws and regulations
B. To identify risk when personal information is collected
C. To ensure senior management has approved the use of personal information
D. To identify threats introduced by business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Which of the following is MOST important to determine as a result of a risk assessment?
A. Process ownership
B. Risk appetite statement
C. Risk tolerance levels
D. Risk response options
Answer: D (LEAVE A REPLY)
Risk response options are the most important factor to determine as a result of a risk assessment, as they involve selecting the optimal strategy and actions to address the identified and assessed risks, and align them with the risk tolerance and appetite of the organization. Process ownership, risk appetite statement, and risk tolerance levels are not the most important factors, as they are more related to the governance, definition, or communication of the risk, respectively, rather than the response to the risk. References = CRISC Review Manual, 7th Edition, page 108.

NEW QUESTION: 200

An organization has determined that risk is not being adequately tracked and managed due to a distributed operating model. Which of the following is the BEST way to address this issue?

Freecram.net

A. Increase the frequency of risk assessments.

B. Create dashboards for risk metrics.

C. Create a centralized portfolio of risk scenarios.

D. Revalidate the organization's risk appetite

Answer: (SHOW ANSWER)

NEW QUESTION: 201

What is the most effective way for a project manager to help mitigate risks throughout the course of a project?

A. Implement project status checks to avoid financial risk.

B. Support the project team in identifying and responding to risk.

C. Update and publish the project risk register on a regular basis.

D. Reduce project cost by eliminating risk to the project.

Answer: (SHOW ANSWER)

The risk management function acts as a consultant and facilitator in IT projects, helping the project team identify, assess, and respond to risks effectively. It does not directly control project status or costs but supports decision-making. Updating risk registers is an operational task often handled by the project team with guidance from risk management. Eliminating all risk is impractical; instead, risks are managed within appetite levels.

NEW QUESTION: 202

A risk practitioner has recently become aware of unauthorized use of confidential personal information within the organization. Which of the following should the risk practitioner do FIRST?

A. Establish database activity monitoring

B. Report the incident to the chief privacy officer (CPO)

C. Invoke the incident response plan

D. Escalate the issue to the data owner

Answer: (SHOW ANSWER)

In the event of a data breach or misuse of confidential information, the first step is to activate the incident response plan. This ensures immediate containment, impact analysis, and communication protocols are followed.

Reference:CRISC Manual - Domain 3, Slide 291-292

NEW QUESTION: 203

Which of the following is the BEST way to validate privileged access to database accounts?

A. Regular reviews of privileged access

B. Confirmation from users with privileged access

C. Management approval of access requests

D. Confirmation from the database administrator (DBA)

Answer: (SHOW ANSWER)

Regular reviewshelp detect inappropriate, outdated, or excessive access rights. This is a fundamental part of access control governance and supports the principle of least privilege.

Reference:CRISC Manual - Domain 1, Slide 230-232

NEW QUESTION: 204

Which of the following would be the GREATEST concern related to data privacy when implementing an Internet of Things (IoT) solution that collects personally identifiable information (PII)?

A. A privacy impact assessment has not been completed.

B. Data encryption methods apply to a subset of PII obtained.

C. The data privacy officer was not consulted.

D. Insufficient access controls are used on the IoT devices.

Answer: D (LEAVE A REPLY)

According to the CRISC Review Manual1, access controls are the policies, procedures, practices, and technologies that are designed and implemented to prevent unauthorized or inappropriate access to IT resources and data. Access controls are essential for ensuring the confidentiality, integrity, and availability of data, especially personally identifiable information (PII), which is any information that can be used to identify, locate, or contact an individual. Insufficient access controls are the greatest concern related to data privacy when implementing an Internet of Things (IoT) solution that collects PII, as they can expose the data to various risks and threats, such as data leakage, theft, loss, corruption, manipulation, or misuse. Insufficient access controls can also cause legal, regulatory, ethical, or reputational issues for the organization, if the data privacy rights and expectations of the individuals are violated or compromised. References = CRISC Review Manual1, page 240, 253.

NEW QUESTION: 205

It is MOST important that security controls for a new system be documented in:

A. testing requirements

B. the implementation plan.

C. System requirements

D. The security policy

Answer: (SHOW ANSWER)

It is most important that security controls for a new system be documented in the system requirements. The system requirements define the functional and non-functional specifications of the system, including the security controls that are needed to protect the system and its data. Documenting the security controls in the system requirements can help ensure that they are designed, developed, tested, and implemented as part of the system development life cycle. Testing requirements, the implementation plan, and the security policy are other documents that may include security controls, but they are not as important as the system requirements. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 5; CRISC Review Manual, 6th Edition, page 212.

NEW QUESTION: 206
Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?
A. Directives from legal and regulatory authorities
B. Audit reports from internal information systems audits
C. Automated logs collected from different systems
D. Trend analysis of external risk factors
Answer: C (LEAVE A REPLY)
Key risk indicators (KRIs) are metrics that help organizations monitor and evaluate the level of risk they are exposed to. They provide early warning signals of potential issues that could affect the achievement of organizational goals12.
The most important data source for monitoring KRIs is automated logs collected from different systems, which are records that capture and store the details and history of the transactions or activities that are performed by the organization's processes, systems, or controls34.
Automated logs collected from different systems are the most important data source because they provide timely and accurate data and information on the performance and status of the organization's operations, and enable the detection and reporting of any deviations, anomalies, or issues that may indicate a risk event34.
Automated logs collected from different systems are also the most important data source because they support the accountability and auditability of the organization's operations, and facilitate the investigation and resolution of any risk event34.
The other options are not the most important data sources, but rather possible inputs or factors that may influence or affect the KRIs. For example:
Directives from legal and regulatory authorities are documents that provide the expectations and obligations of the external authorities or bodies that govern or oversee the organization's activities and operations, such as laws, regulations, standards, or contracts5 . However, these documents are not the most important data source becausethey do not directly measure or monitor the level of risk exposure, but rather provide the criteria or framework for risk compliance5 .
Audit reports from internal information systems audits are documents that provide the findings and recommendations of the independent and objective assessment of the adequacy and effectiveness of the organization's information systems, processes, and controls . However, these documents are not the most important data source because they do not directly measure or monitor the level of risk exposure, but rather provide the assurance or improvement for risk management .
Trend analysis of external risk factors is a technique that involves analyzing and forecasting the changes and impacts of the external factors that influence the organization's operations, such as technology, competition, regulation, or customer behavior . However, this technique is not the most important data source because it does not directly measure or monitor the level of risk exposure, but rather provide the insight or prediction for risk identification . References =
1: Key Risk Indicators: A Practical Guide | SafetyCulture1
2: Key risk indicator - Wikipedia2
3: Database Activity Monitoring - Wikipedia3
4: Database Activity Monitoring (DAM) | Imperva4

5: Regulatory Compliance - Wikipedia5
Regulatory Compliance Management Software | MetricStream
IT Audit and Assurance Standards, ISACA, 2014
IT Audit and Assurance Guidelines, ISACA, 2014
Trend Analysis - Investopedia
Trend Analysis: A Definition and Examples

NEW QUESTION: 207
Which of the following roles should be assigned accountability for monitoring risk levels?
A. Risk practitioner
B. Business manager
C. Risk owner
D. Control owner
Answer: C (LEAVE A REPLY)
The risk owner should be assigned accountability for monitoring risk levels, as they have the authority and responsibility to manage the risk and its associated controls, and to report on the risk status and performance.
The risk practitioner, the business manager, and the control owner are not the best choices, as they have different roles and responsibilities related to risk identification, assessment, response, and reporting, but they are not accountable for the risk and its monitoring. References = CRISC Review Manual, 7th Edition, page 101.

NEW QUESTION: 208
When outsourcing a business process to a cloud service provider, it is MOST important to understand that:
A. insurance could be acquired for the risk associated with the outsourced process.
B. service accountability remains with the cloud service provider.
C. a risk owner must be designated within the cloud service provider.
D. accountability for the risk will remain with the organization.
Answer: (SHOW ANSWER)
According to the FIC Article by FSCA, accountable institutions remain fully accountable, responsible and liable for any compliance failures that may result from or be associated with an outsourcing arrangement and as such, liability and/or culpability for non-compliance with the FIC Act obligations cannot be transferred to a third-party service provider2. Therefore, even if a business process is outsourced to a cloud service provider, the organization still has the ultimate responsibility and accountability for the risk associated with the outsourced process. The other options are not correct, as they imply that the cloud service provider can take over the accountability or responsibility for the risk, or that the organization can mitigate the risk by acquiring insurance, which is not the case.

NEW QUESTION: 209
Which of the following provides the BEST indication that existing controls are effective?
A. Control testing

B. Control logging
C. Control documentation
D. Control design
Answer: (SHOW ANSWER)
Control effectiveness is best determined throughcontrol testing, which evaluates whether a control operates as intended over time. It includes functional and operational validation under real-world conditions, unlike documentation or design, which only indicate intent.
Reference:CRISC Manual - Domain 4, Slide 388-390

NEW QUESTION: 210
Which of the following should an organization perform to forecast the effects of a disaster?
A. Develop a business impact analysis (BIA).
B. Define recovery time objectives (RTO).
C. Analyze capability maturity model gaps.
D. Simulate a disaster recovery.
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of a disaster on the critical functions and processes of an organization1. A BIA helps to forecast the operational, financial, legal, and reputational impacts of a disaster, as well as the recovery priorities and resources needed to resume normal operations2. A BIA also helps to determine the recovery time objectives (RTO), which are the maximum acceptable time frames for restoring the critical functions and processes after a disaster3. Therefore, developing a BIA is the most important step for an organization to forecast the effects of a disaster and plan for its recovery. Defining RTOs is a part of the BIA process, not a separate activity. Analyzing capability maturity model gaps is a method to assess the effectiveness and efficiency of the organization's processes and practices, but it does not directly forecast the effects of adisaster4. Simulating a disaster recovery is a way to test and validate the recovery plans and procedures, but it does not forecast the effects of a disaster either5. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk Response and Mitigation, Section 5.3: Business Continuity Planning, pp. 227-238.

NEW QUESTION: 211
An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?
A. Redesign the heat map.
B. Review the risk tolerance.
C. Perform a business impact analysis (BIA)
D. Update the risk register.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, the risk register is a tool that records the results of risk identification, analysis, evaluation, and treatment. It should be updated whenever there is a change in the risk profile, such as when a vulnerability is closed or a new threat is identified. Updating the risk register allows the organization to monitor the current status of risks and the effectiveness of risk responses.

Therefore, the next course of action after implementing changes to close an identified vulnerability is to update the risk register with the new information. References = CRISC Review Manual1, page 191.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 212
A threat intelligence team has identified an indicator of compromise related to an advanced persistent threat (APT) actor. Which of the following is the risk practitioner's BEST course of action?
A. Review the most recent vulnerability scanning report.
B. Determine the adequacy of existing security controls.
C. Determine the business criticality of the asset.
D. Review prior security incidents related to the asset.
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Which of the following provides the BEST evidence that a selected risk treatment plan is effective?
A. Identifying key risk indicators (KRIs)
B. Evaluating the return on investment (ROI)
C. Evaluating the residual risk level
D. Performing a cost-benefit analysis
Answer: (SHOW ANSWER)
A risk treatment plan is a document that describes the actions and resources required to implement the chosen risk response for a specific risk scenario. A risk response can be to accept, avoid, transfer, or mitigate the risk.
The effectiveness of a risk treatment plan can be measured by how well it reduces the risk exposure and achieves the desired outcomes. The best evidence that a selected risk treatment plan is effective is to evaluate the residual risk level, which is the remaining risk after the risk treatment plan has been implemented. The residual risk level should be within the organization's risk appetite and tolerance, and should reflect the actual risk reduction and value creation of the risk treatment plan. Evaluating the residual risk level can also help to identify any gaps or issues that need to be addressed, and to monitor and report on the risk performance and improvement. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.2, p.
108-109

NEW QUESTION: 214

Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

A. Chief financial officer

B. Information security director

C. Internal audit director

D. Chief information officer

Answer: (SHOW ANSWER)

The chief information officer (CIO) is the most likely person to be responsible for the coordination between the IT risk strategy and the business risk strategy, because the CIO is the senior executive who oversees the information technology (IT) function and aligns it with the organization's strategy, objectives, and operations. The CIO is also responsible for ensuring that the IT function delivers value, supports innovation, and manages IT risks effectively and efficiently. The CIO can coordinate the IT risk strategy and the business risk strategy by communicating and collaborating with other business leaders, establishing and implementing IT governance frameworks and policies, and monitoring and reporting on IT performance and risk indicators.

The other options are not as likely as the CIO to be responsible for the coordination between the IT risk strategy and the business risk strategy, because they have different or limited roles and responsibilities in relation to IT and business risk management, as explained below:

A: Chief financial officer (CFO) is the senior executive who oversees the financial function and manages the financial risks of the organization. The CFO may be involved in the coordination between the IT risk strategy and the business risk strategy, especially when it comes to budgeting, funding, or reporting on IT-related projects and initiatives, but the CFO is not the primary person who oversees the IT function and aligns it with the organization's strategy and objectives.

B: Information security director is the senior manager who oversees the information security function and manages the information security risks of the organization. The information security director may be involved in the coordination between the IT risk strategy and the business risk strategy, especially when it comes to protecting the confidentiality, integrity, and availability of the information assets and systems, but the information security director is not the primary person who oversees the IT function and aligns it with the organization's strategy and objectives.

C: Internal audit director is the senior manager who oversees the internal audit function and provides independent assurance on the effectiveness and efficiency of the organization's governance, risk management, and control processes. The internal audit director may be involved in the coordination between the IT risk strategy and the business risk strategy, especially when it comes to auditing, reviewing, or testing the IT- related processes and controls, but the internal audit director is not the primary person who oversees the IT function and aligns it with the organization's strategy and objectives. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.1.1, page 7. The Strategic CIO: Balancing Business and IT Priorities, Technology's Role in Enterprise Risk Management, Aligning Enterprise Cyber Risk and Business Strategy

NEW QUESTION: 215

Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

A. The number of stakeholders involved in IT risk identification workshops

B. The percentage of corporate budget allocated to IT risk activities
C. The percentage of incidents presented to the board
D. The number of executives attending IT security awareness training
Answer: (SHOW ANSWER)
The best indicator of executive management's support for IT risk mitigation efforts is the number of executives attending IT security awareness training. This shows that the executives are committed to enhancing their knowledge and skills on IT security issues, and that they are setting a positive example for the rest of the organization. The number of stakeholders involved in IT risk identification workshops, the percentage of corporate budget allocated to IT risk activities, and the percentage of incidents presented to the board are other possible indicators, but they are not as strong as the number of executives attending IT security awareness training. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 7; CRISC Review Manual, 6th Edition, page 202.

NEW QUESTION: 216
An organization is subject to a new regulation that requires nearly real-time recovery of its services following a disruption. Which of the following is the BEST way to manage the risk in this situation?
A. Move redundant IT infrastructure to a closer location.
B. Obtain insurance and ensure sufficient funds are available for disaster recovery.
C. Review the business continuity plan (BCP) and align it with the new business needs.
D. Outsource disaster recovery services to a third-party IT service provider.
Answer: (SHOW ANSWER)
Updating the BCP to align with real-time recovery requirements ensures the organization's resilience to disruptions while meeting regulatory standards. This action reflects Business Continuity and Disaster Recovery Planning best practices.

NEW QUESTION: 217
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:
A. that results in a full root cause analysis.
B. used for verification within the SLA.
C. that are verified as actual incidents.
D. resolved within the SLA.
Answer: (SHOW ANSWER)
When establishing leading indicators for the information security incident response process, it is most important to consider the percentage of reported incidents that are resolved within the service level agreement (SLA). A leading indicator is a metric that can predict or influence the future performance or outcome of a process or activity. A leading indicator for the information security incident response process should measure how well the process is achieving its objectives, such as minimizing the impact of incidents, restoring normal operations as quickly as possible, and preventing recurrence of incidents. The percentage of reported incidents that are resolved within the SLA is a leading indicator that reflects the efficiency and effectiveness of the information security incident response process. It shows how well the process is meeting

the expectations and requirements of the stakeholders, such as the business units, customers, and regulators. It also shows how well the process is managing the resources, such as time, budget, and personnel, that are allocated for incident response. A high percentage of reported incidents that are resolved within the SLA indicates that the information security incident response process is performing well and delivering value to the organization. A low percentage of reported incidents that are resolved within the SLA indicates that the information security incident response process is facing challenges and needs improvement. The percentage of reported incidents that are resolved within the SLA can also help identify the root causes of incidents, the gaps in the process, and the areas for improvement. For example, if the percentage of reported incidents that are resolved within the SLA is low, it may indicate that the process has issues with the following aspects: - Incident detection and reporting: The process may not have adequate tools, techniques, or procedures to detect and report incidents in a timely and accurate manner. - Incident prioritization and classification: The process may not have clear and consistent criteria to prioritize and classify incidents based on their severity, impact, and urgency. - Incident analysis and investigation: The process may not have sufficient skills, knowledge, or evidence to analyze and investigate the incidents and determine their root causes, scope, and consequences. - Incident containment and eradication: The process may not have effective methods or measures to contain and eradicate the incidents and prevent them from spreading or escalating. - Incident recovery and restoration: The process may not have reliable backup and recovery plans or systems to restore the normal operations and functionality of the affected systems or services. - Incident communication and escalation: The process may not have proper communication and escalation channels or protocols to inform and involve the relevant stakeholders, such as the management, the users, the vendors, or the authorities. - Incident documentation and closure: The process may not have adequate documentation and closure procedures to record and report the incidents and their resolution. - Incident review and improvement: The process may not have regular review and improvement activities to evaluate and enhance the process and its performance. Therefore, the percentage of reported incidents that are resolved within the SLA is the most important leading indicator for the information security incident response process, as it can provide valuable insights and feedback for the process and its improvement. References = Information Security Incident Response | Process Street1, Key Performance Indicators (KPIs) for Security Operations and Incident Response2, 7 Incident Response Metrics and How to Use Them3

NEW QUESTION: 218

A data processing center operates in a jurisdiction where new regulations have significantly increased penalties for data breaches. Which of the following elements of the risk register is MOST important to update to reflect this change?

A. Risk impact

B. Risk trend

C. Risk appetite

D. Risk likelihood

Answer: A (LEAVE A REPLY)

Risk impact is the potential loss or damage that a risk event can cause to an organization. Risk impact can be expressed in qualitative or quantitative terms, such as financial, reputational, operational, or legal. A risk register is a tool that records and tracks the key information about the identified risks, such as their

description, likelihood, impact, response, and status. A risk register helps an organization to monitor and manage its risks effectively and efficiently. When there is a change in the external or internal environment that affects the organization's risks, such as new regulations, the risk register should be updated to reflect this change. The most important element of the risk register to update in this case is the risk impact, because the new regulations have significantly increased the penalties for data breaches, which means that the potential loss or damage that a data breach can cause to the organization has also increased. By updating the risk impact, the organization can reassess the severity and priority of the data breach risk, and adjust its risk response accordingly. The other elements of the risk register are less important to update in this case. The risk trend shows the direction and rate of change of the risk over time, which may or may not be affected by the new regulations. The risk appetite is the amount and type of risk that the organization is willing to accept in pursuit of its objectives, which is unlikely to change due to the new regulations. The risk likelihood is the probability of a risk event occurring, which is also independent of the new regulations. References = Risk IT Framework, ISACA, 2022, p. 131

NEW QUESTION: 219

Which of the following BEST promotes commitment to controls?

A. Assigning control ownership

B. Assigning appropriate resources

C. Assigning a quality control review

D. Performing regular independent control reviews

Answer: (SHOW ANSWER)

Commitment to controls is the degree to which the organization and its stakeholders support and adhere to the controls that are designed and implemented to manage or mitigate the risks1. Commitment to controls is essential for ensuring the effectiveness and efficiency of the controls, as well as the achievement of the organization's objectives and strategies2. The best way to promote commitment to controls is to assign control ownership, which is the process of identifying and assigning the person or entity that has the authority and accountability for a control and its management3. By assigning control ownership, the organization can ensure that the controls are properly and promptly designed, implemented, monitored, and maintained, and that the issues or gaps in the controls are identified andresolved4. Assigning control ownership also helps to establish and communicate the roles and responsibilities of the control owners and the other stakeholders, and to enforce the accountability and performance of the control owners5. Assigning appropriate resources, assigning a quality control review, and performing regular independent control reviews are not the best ways to promote commitment to controls, as they do not provide the same level of authority and accountability as assigning control ownership. Assigning appropriate resources is the process of allocating and providing the necessary funds, staff, equipment, or technology that are required to support or enable the controls. Assigning appropriate resources can enhance the quality and performance of the controls, but it does not ensure that the controls are managed or maintained by a specific person or entity. Assigning a quality control review is the process of conducting and documenting a systematic and objective examination and evaluation of the controls, to ensure that they meet the established standards and requirements. Assigning a quality control review can improve the reliability and compliance of the controls, but it does not ensure that the controls are owned or operated by a specific person or entity. Performing regular independent control

reviews is the process of performing and reporting an independent and impartial assessment and verification of the controls, to provide assurance and advice on the adequacy and effectiveness of the controls. Performing regular independent control reviews can provide feedback and recommendations for the controls, but it does notensure that the controls are implemented or improved by a specific person or entity. References = 1: Commitment Controls - IMF2: 17 COSO Principles of Effective Internal Control | Weaver3: [Control Ownership - ISACA] 4: [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.1: Control Design, pp. 233-235.] 5: [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.2: Control Implementation, pp. 243-245.] : Resource Allocation - an overview | ScienceDirect Topics : Quality Control Review - an overview | ScienceDirect Topics : IT Risk Resources | ISACA : [Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.1: Risk Identification, pp. 57-59.] : [Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.3: Control Monitoring and Maintenance, pp. 251-253.]

NEW QUESTION: 220

The number of tickets to rework application code has significantly exceeded the established threshold.
Which of the following would be the risk practitioner's BEST recommendation?

Freecram.net

A. Perform a root cause analysis
B. Perform a code review
C. Implement version control software.
D. Implement training on coding best practices
Answer: (SHOW ANSWER)
A root cause analysis is a process of identifying and understanding the underlying or fundamental causes or factors that contribute to or result in a problem or incident that has occurred or may occur in the organization. A root cause analysis can provide useful insights and solutions on the origin and nature of the problem or incident, and prevent or reduce its recurrence or impact.
Performing a root cause analysis is the risk practitioner's best recommendation when the number of tickets to rework application code has significantly exceeded the established threshold, because it can help the organization to address the following questions:
Why did the application code require rework?
What were the errors or defects in the application code?
How did the errors or defects affect the functionality or usability of the application?
Who was responsible or accountable for the application code development and testing?
When and how were the errors or defects detected and reported?
What were the costs or consequences of the rework for the organization and its stakeholders?
How can the errors or defects be prevented or minimized in the future?
Performing a root cause analysis can help the organization to improve and optimize the application code quality and performance, and to reduce or eliminate the need for rework. It can also help the organization to

align the application code development and testing with the organization's objectives and requirements, and to comply with the organization's policies and standards.
The other options are not the risk practitioner's best recommendations when the number of tickets to rework application code has significantly exceeded the established threshold, because they do not address the main purpose and benefit of performing a root cause analysis, which is to identify and understand the underlying or fundamental causes or factors that contribute to or result in the problem or incident.
Performing a code review is a process of examining and evaluating the application code for its quality, functionality, and security, using the input and feedback from the peers, experts, or tools. Performing a code review can help the organization to identify and resolve the errors or defects in the application code, but it is not the risk practitioner's best recommendation, because it does not indicate why the application code required rework, and how the errors or defects affected the organization and its stakeholders.
Implementing version control software is a process of using a software tool to manage and track the changes and modifications to the application code, and to ensure the consistency and integrity of the application code. Implementing version control software can help theorganization to control and monitor the application code development and testing, but it is not the risk practitioner's best recommendation, because it does not indicate why the application code required rework, and how the errors or defects affected the organization and its stakeholders.
Implementing training on coding best practices is a process of providing and facilitating the learning and development of the skills and knowledge on the principles, guidelines, and standards for the application code development and testing. Implementing training on coding best practices can help the organization to enhance the competence and performance of the application code developers and testers, but it is not the risk practitioner's best recommendation, because it does not indicate why the application code required rework, and how the errors or defects affected the organization and its stakeholders. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 40-41, 47-48, 54-55, 58-59, 62-63 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 189 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 221
A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?
A. The contingency plan provides for backup media to be taken to the alternative site.
B. The contingency plan for high priority applications does not involve a shared cold site.
C. The alternative site is a hot site with equipment ready to resume processing immediately.
D. The alternative site does not reside on the same fault no matter how far the distance apart.
Answer: D (LEAVE A REPLY)
The most important consideration when establishing a contingency plan and an alternate processing site for a company that has located its computer center on a moderate earthquake fault is that the alternative site does not reside on the same fault no matter how far the distance apart, as it ensures that the alternative site is not affected by the same earthquake event that may disrupt the primary site, and that the business continuity and recovery objectives can be met. The other options are not the most important considerations, as they are more related to the backup, priority, or readiness of the alternative site, respectively, rather than the location of the alternative site. References = CRISC Review Manual, 7th Edition, page 111.

NEW QUESTION: 222
Which of the following is the PRIMARY reason that risk management is important in project management?
A. It helps identify and mitigate potential issues that could derail projects.
B. It helps to ensure project acceptance by end users.
C. It reduces the risk associated with potential project scope creep.
D. It facilitates agreement and collaboration on project goals among stakeholders.
Answer: A (LEAVE A REPLY)
Risk management in project management is crucial for identifying and mitigating potential issues that could jeopardize project success. By proactively addressing risks, project managers can ensure that projects are completed on time, within budget, and meet quality standards.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 1: Governance, Section: Risk Management in Project Management.

NEW QUESTION: 223
An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:
A. rolled back changes below management's thresholds.
B. change-related exceptions per month.
C. the average implementation time for changes.
D. number of user stories approved for implementation.
Answer: (SHOW ANSWER)
= Change management is the process of planning, implementing, and monitoring changes to IT systems, services, or infrastructure in a controlled and coordinated manner1. Change management controls are the policies, procedures, and tools that ensure changes are authorized, documented, tested, and reviewed before they are deployed to the production environment2.
Change-related exceptions are the deviations or violations from the established change management controls, such as unauthorized, untested, or failed changes3. Change-related exceptions pose a high risk to theorganization, as they can cause system instability, performance degradation, security breaches, data loss, or compliance issues3.
An increase in change-related exceptions per month would be the greatest concern for an IT risk practitioner, as it indicates a lack of effectiveness, efficiency, or compliance of the change management process and controls. An increase in change-related exceptions per month could result from:
Poor change planning, prioritization, or scheduling
Insufficient change approval, review, or communication
Inadequate change testing, validation, or verification
Lack of change monitoring, reporting, or auditing
Low change awareness, training, or support
An IT risk practitioner should investigate the root causes of the increase in change-related exceptions per month, and recommend corrective and preventive actions to improve the change management process and controls, such as:

Aligning the change management process with the organization's goals, strategies, and risk appetite Implementing a standardized and consistent change management methodology, such as ITIL or COBIT Defining clear roles and responsibilities for change management stakeholders, such as change owners, change managers, change advisory boards, change implementers, and change users Establishing clear and measurable criteria and thresholds for change authorization, classification, and evaluation Leveraging tools and technologies to automate and streamline the change management process and controls, such as change management software, configuration management databases, or change management dashboards Enhancing the change management culture and capabilities, such as change management awareness, training, support, or feedback The other options are not as concerning as an increase in change-related exceptions per month, because they do not directly imply a risk to the organization's IT systems, services, or infrastructure. Rolled backchanges below management's thresholds, which are the changes that are reversed or undone due to errors, defects, or issues, may indicate a need for improvement in the change testing, validation, or verification processes, but they do not necessarily cause harm or damage to the production environment, as long as they are within the acceptable limits set bythe management. The average implementation time for changes, which is the duration of the change deployment process, may affect the organization's agility, efficiency, or productivity, but it does not necessarily compromise the quality, security, or reliability of the changes, as long as they are implemented according to the change management controls. The number of user stories approved for implementation, which are the requirements or features that are expressed from the perspective of the end users, may reflect the organization's demand, innovation, or customer satisfaction, but it does not necessarily increase the risk of the changes, as long as they are managed and controlled by the change management process.
References = What is Change Management? | ITIL | AXELOS, Change Management Controls: Definition, Types, and Best Practices, Change Management Exceptions: Definition, Causes, and Impacts, ITIL Change Management: Best Practices & Processes - BMC Software, COBIT 2019: Change Enablement

NEW QUESTION: 224
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?
A. Several risk action plans have missed target completion dates.
B. Senior management has accepted more risk than usual.
C. Risk associated with many assets is only expressed in qualitative terms.
D. Many risk scenarios are owned by the same senior manager.
Answer: (SHOW ANSWER)
The most concerning issue for a risk practitioner reviewing an organization risk register is that several risk action plans have missed target completion dates. This indicates that the risk responses are not being implemented effectively or timely, and that the risk exposure may not be reduced as expected. Senior management accepting more risk than usual, risk associated with many assets being expressed in qualitative terms, and many risk scenarios being owned by the same senior manager are not as concerning as the missed deadlines, as they may reflect the risk appetite, tolerance, and culture of the organization.
References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 10; CRISC Review Manual, 6th Edition, page 140.

NEW QUESTION: 225
Which of the following would be MOST helpful in assessing the risk associated with data loss due to human vulnerabilities?
A. Reviewing password change history
B. Performing periodic access recertification
C. Conducting social engineering exercises
D. Reviewing the results of security awareness surveys
Answer: (SHOW ANSWER)
Social engineering exercises are simulations of real-world attacks that exploit human vulnerabilities, such as phishing, baiting, pretexting, or quid pro quo. Conducting social engineering exercises can help assess the risk associated with data loss due to human vulnerabilities by measuring the employees' susceptibility to such attacks, their awareness of security policies and procedures, and their response to incidents. Reviewing password change history, performing periodic access recertifications, and reviewing the results of security awareness surveys are also useful, but they do not directly test the employees' behavior and resilience in the face of social engineering attacks.

NEW QUESTION: 226
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?
A. An antivirus program
B. Database activity monitoring
C. Firewall log monitoring
D. File integrity monitoring
Answer: (SHOW ANSWER)
Zero-day malware is malware that exploits unknown and unprotected vulnerabilities. This novel malware is difficult to detect and defend against, making zero-day attacks a significant threat to enterprise cybersecurity1. The best way to detect zero-day malware on an end user's workstation is to use file integrity monitoring, which is a technique that monitors and alerts on changes to files and directories that may indicate a malware infection or compromise2. By using file integrity monitoring, the end user can detect zero-day malware that may alter or damage the files or directories on their workstation, and take appropriate actions to remove or isolate the malware. File integrity monitoring can also help to prevent the spread of zero-day malware to other systems or networks, and to restore the integrity and availability of the affected files or directories. Antivirus program, database activity monitoring, and firewall log monitoring are not the best ways to detect zero-day malware on an end user's workstation, as they are not as effective or reliable as file integrity monitoring. Antivirus program is a software that scans and removes known malware from a system or network3. Antivirus program can help to protect the end user's workstation from common or known malware, but it may not be able to detect zero-day malware that does not have a signature or a pattern that matches the antivirus program's database. Database activity monitoring is a technique that monitors and audits the activities and transactions on a database, such as queries, updates, or deletions4. Database activity monitoring can help to protect the end user's database from unauthorized or malicious access or modification, but it may not be able to detect zero-day malware that does not target or affect the database.

Firewall log monitoring is a technique that monitors and analyzes the logs generated by a firewall, which is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. Firewall log monitoring can help to protect the end user's workstation from external or internal network attacks, but it may not be able to detect zero-day malwarethat bypasses or evades the firewall rules or that originates from the workstation itself. References = 1: What is Zero Day Malware? - Check Point Software2: File Integrity Monitoring - an overview | ScienceDirect Topics3: Antivirus Software - an overview | ScienceDirect Topics4: Database Activity Monitoring - an overview | ScienceDirect Topics : [Firewall Log Analysis - an overview | ScienceDirect Topics] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.1: Control Design, pp. 233-235.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.2: Control Implementation, pp. 243-245.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.3: Control Monitoring and Maintenance, pp. 251-253.] : [Zero-day attack detection: a systematic literature review | Artificial Intelligence Review] : [Zero-day Attacks Detection and Prevention Methods | Apriorit]

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?
A. Obtain necessary resources to address regulatory requirements
B. Develop a policy framework that addresses regulatory requirements
C. Perform a gap analysis against regulatory requirements.
D. Employ IT solutions that meet regulatory requirements.
Answer: (SHOW ANSWER)
The most important step to ensure regulatory requirements are adequately addressed within an organization is to develop a policy framework that addresses regulatory requirements. A policy framework is a set of principles, rules, and standards that guide the organization's actions and decisions. By developing a policy framework that addresses regulatory requirements, the organization can establish a clear and consistent direction, expectation, and accountability for complying with the relevant laws and regulations. Obtaining necessary resources, performing a gap analysis, and employing IT solutions are other possible steps, but they are not as important as developing a policy framework. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 4; CRISC Review Manual, 6th Edition, page 153.

NEW QUESTION: 228
In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?
A. Risk questionnaire
B. Risk register
C. Management assertion
D. Compliance manual
Answer: (SHOW ANSWER)
A risk register is a tool that records and tracks the risks that may affect the organization, as well as the actions that are taken or planned to manage them1. A risk register provides the best evidence that the IT risk profile is up to date, because it reflects the current and potential IT risks that the organization faces, as well as their likelihood, impact, severity, owner, status, and response2. An IT risk profile is a document that describes the types, amounts, and priority of IT risk that the organization finds acceptable and unacceptable3. An IT risk profile is developed collaboratively with various stakeholders within the organization, including business leaders, data and process owners, enterprise risk management, internal and external audit, legal, compliance, privacy, and IT risk management and security4. By maintaining and updating the risk register regularly, the organization can ensure that the IT risk profile is aligned with the changing IT risk environment, and that the IT risk management activities and performance are consistent and effective. The other options are not the best evidence that the IT risk profile is up to date, as they are either less comprehensive or less relevant than the risk register. A risk questionnaire is a tool that collects and analyzes the opinions and perceptions of the stakeholders about the risks that may affect the organization5. A risk questionnaire can help to identify and assess the risks, as well as to communicate and report on the risk status and issues. However, a risk questionnaire is not the best evidence that the IT risk profile is up to date, as it may not capture all the IT risks that the organization faces, or reflect the actual or objective level and nature of the IT risks. A management assertion is a statement or declaration made by the management about the accuracy and completeness of the information or data that they provide or report. A management assertion can help to increase the confidence and trust of the stakeholders and auditors in the information or data, as well as to demonstrate the accountability and responsibility of the management. However, a management assertion is not the best evidence that the IT risk profile is up to date, as it does not provide the details or outcomes of the IT risk management activities or performance, or verify the validity and reliability of the IT risk information or data.
A compliance manual is a document that contains the policies, procedures, and standards that the organization must follow to meet the legal, regulatory, or contractual requirements that apply to its activities or operations.
A compliance manual can help to ensure the quality and consistency of the organization's compliance activities or performance, as well as to avoid or reduce the penalties or sanctions for non-compliance. However, a compliance manual is not the best evidence that the IT risk profile is up to date, as it does not address the IT risks that the organization faces, or the IT risk management activities or performance.
References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.5, Page 55.

NEW QUESTION: 229
Which of the following is MOST important for successful incident response?
A. The quantity of data logged by the attack control tools
B. Blocking the attack route immediately
C. The ability to trace the source of the attack
D. The timeliness of attack recognition
Answer: (SHOW ANSWER)
The most important factor for successful incident response is the timeliness of attack recognition. Incident response is the process of detecting, analyzing, containing, eradicating, recovering, and reporting on security incidents that could affect the organization's IT systems or data. The timeliness of attack recognition is the speed and accuracy with which the organization can identify and confirm that an attack has occurred or is in progress. The timeliness of attack recognition is crucial for successful incident response, as it affects the ability and effectiveness of the organization to respond to and mitigate the attack, and to minimize the damage and impact of the attack. The other options are not as important as the timeliness of attack recognition, although they may also contribute to or influence the incident response. The quantity of data logged by the attack control tools, the ability to trace the source of the attack, and the blocking of the attack route immediately are all factors that could help or hinder the incident response, but they are not the most important factor for successful incident response. References = CISA Review Manual, 27th Edition, Chapter 5, Section
5.4.1, page 5-32.

NEW QUESTION: 230
What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

ISACA® freecram.net

A. Relative positions on the risk map
B. Risk treatment options
C. Capability of enterprise to implement
D. The multiple risk factors addressed by a chosen response
Answer: (SHOW ANSWER)
The risk scenario chart shows the initial and residual risk ratings, and the project cost, for four projects named Sierra, Tango, Uniform, and Victor. The initial risk rating is the level of risk before applying any controls or mitigation measures, while the residual risk rating is the level of risk after applying the controls or measures.

The project cost is the amount of resources required to implement the project. These three factors can be used to determine the relative positions of the projects on a risk map, which is a graphical tool for displaying the risks based on their impact and likelihood. The risk map can help to prioritize and compare the risks, and to select the most appropriate risk response strategy. The other options are not the best answers, as they are not directly shown or derived from the risk scenario chart. The risk treatment options are the possible actions that can be taken to address the risks, such as accept, avoid, mitigate, or transfer. The capability of enterprise to implement is the ability of the organization to execute the risk response plan,considering the available resources, skills, and constraints. The multiple risk factors addressed by a chosen response are the various elements that contribute to or affect the risk, such as the threat sources, events, vulnerabilities, assets, and impacts. These factors are not explicitly stated or measured in the risk scenario chart, and may require further analysis or information. References = How to Write Strong Risk Scenarios and Statements - ISACA; Identifying the Right Risk Scenarios to Measure with FAIR; How to write good risk scenarios and statements

NEW QUESTION: 231
Which of the following BEST indicates that an organizations risk management program is effective?
A. Fewer security incidents have been reported.
B. The number of audit findings has decreased.
C. Residual risk is reduced.
D. inherent risk Is unchanged.
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after the implementation of risk responses. An effective risk management program should aim to reduce the residual risk to a level that is acceptable by the enterprise, in alignment with its risk appetite and tolerance. The reduction of residual risk indicates that the risk responses are appropriate and effective, and that the enterprise is achieving its objectives while managing its risks. The other options are not necessarily indicative of an effective risk management program, as they may depend on other factors, such as the reporting culture, the audit scope and methodology, and the nature and source of the inherent risk. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section
1.2.3.1, pp. 24-25.

NEW QUESTION: 232
Which of the following is the BEST recommendation when a key risk indicator (KRI) is generating an excessive volume of events?
A. Reevaluate the design of the KRIs.
B. Develop a corresponding key performance indicator (KPI).
C. Monitor KRIs within a specific timeframe.
D. Activate the incident response plan.
Answer: (SHOW ANSWER)
Reevaluating the design of the key risk indicators (KRIs) is the best recommendation when a KRI is generating an excessive volume of events, because it helps to determine whether the KRI is relevant,

reliable, and valid, and whether it needs to be modified or replaced. A KRI is a metric or indicator that helps to monitor and evaluate the likelihood or impact of a risk, or the effectiveness or efficiency of a control. A KRI can be quantitative or qualitative, and can be derived from internal or external sources. An event is an occurrence or incident that may indicate a change or trend in the risk level or performance. A KRI that generates an excessivevolume of events may indicate that the KRI is not well-designed or well-aligned with the risk objectives or criteria, and that it may produce false positives or negatives, or irrelevant or misleading information. Therefore, reevaluating the design of the KRIs is the best recommendation, as it helps to improve the quality and usefulness of the KRIs, and to avoid unnecessary or inappropriate actions or responses.
Developing a corresponding key performance indicator (KPI), monitoring KRIs within a specific timeframe, and activating the incident response plan are all possible actions to perform after reevaluating the design of the KRIs, but they are not the best recommendation, as they do not address the root cause of the excessive volume of events. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.3.2, page 97

NEW QUESTION: 233
Which of the following BEST enables detection of ethical violations committed by employees?
A. Transaction log monitoring
B. Access control attestation
C. Periodic job rotation
D. Whistleblower program
Answer: D (LEAVE A REPLY)
Whistleblower Program:
Definition: A whistleblower program allows employees to report unethical or illegal activities within the organization anonymously.
Detection of Ethical Violations: Employees are often in the best position to observe unethical behavior. A well-structured whistleblower program encourages them to report such behavior without fear of retaliation.
Anonymity and Protection: Providing anonymity and protection to whistleblowers increases the likelihood that employees will report violations, thus enabling the organization to detect and address ethical issues more effectively.
Comparison with Other Options:
Transaction Log Monitoring: While useful for detecting anomalies and potential fraud, it is not specifically focused on ethical violations and may not capture all types of unethical behavior.
Access Control Attestation: This ensures that users have the correct access permissions but does not directly detect unethical behavior.
Periodic Job Rotation: This can help prevent fraud by reducing the risk of collusion and providing fresh perspectives on processes, but it does not directly detect ethical violations.
Best Practices:
Clear Reporting Channels: Ensure that the whistleblower program has clear and accessible reporting channels.

Training and Awareness: Regularly train employees on the importance of reporting unethical behavior and the protections offered by the whistleblower program.
Follow-up and Action: Ensure that reports are investigated thoroughly and appropriate actions are taken to address verified violations.
References:
CRISC Review Manual: Emphasizes the importance of ethical behavior and the role of whistleblower programs in detecting and addressing ethical violations within organizations.
ISACA Guidelines: Support the implementation of whistleblower programs as a key component of a comprehensive risk management and ethical governance framework.

NEW QUESTION: 234
An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?
A. Develop key risk indicators (KRIs).
B. Ensure sufficient pre-implementation testing.
C. Identify applicable risk scenarios.
D. Identify the organization's critical data.
Answer: (SHOW ANSWER)
Artificial intelligence (AI) is a branch of computer science that aims to create machines or systems that can perform tasks that normally require human intelligence, such as learning, reasoning, decision making, etc. An organization that is considering adopting AI should be aware of the potential risks and challenges that may arise from using AI, such as ethical, legal, social, technical, operational, or security issues.
The most important course of action for the risk practitioner is to identify applicable risk scenarios. This means that the risk practitioner should analyze the context and objectives of the AI adoption, the stakeholders and their expectations, the data and information sources and quality, the AI models and algorithms and their reliability, the AI outputs and outcomes and their impact, and the AI governance and oversight mechanisms and their effectiveness.
Identifying applicable risk scenarios helps to assess the likelihood and impact of the risks, prioritize the risks, design and implement appropriate risk responses, monitor and evaluate the risk performance, and report and communicate the risk status and issues.
The other options are not the most important courses of action for the risk practitioner. They are either secondary or not essential for AI risk management.
The references for this answer are:
Risk IT Framework, page 24
Information Technology & Security, page 18
Risk Scenarios Starter Pack, page 16

NEW QUESTION: 235
Which of the following is the BEST method to track asset inventory?
A. Periodic asset review by management
B. Asset registration form

C. Automated asset management software
D. IT resource budgeting process
Answer: (SHOW ANSWER)
Automated asset management software is the best method to track asset inventory because it can provide real-time, accurate, and comprehensive data on the location, condition, value, and usage of assets. It can also help to optimize asset utilization, reduce costs, improve compliance, and enhance security.
References
*Free Asset Tracking Templates | Smartsheet
*5 Best Asset Management Software (2023) - Forbes Advisor
*What Is Asset Tracking? Benefits & How It Works - Forbes
*Inventory and Asset Tracking: Keep it Simple (But Powerful)

NEW QUESTION: 236
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors
A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases
C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours
Answer: (SHOW ANSWER)
Software as a Service (SaaS) is a cloud computing model that provides software applications over the internet, without requiring the users to install or maintain them on their own devices. SaaS vendors are responsible for hosting, managing, and updating the software applications, and providing technical support and security to the users. The key performance indicator (KPI) that would best measure the risk of a service outage when using a SaaS vendor is the frequency and duration of unplanned downtime, which is the amount and length of time that the software applications are unavailable or inaccessible due to unexpected events, such as network failures, server crashes, power outages, cyberattacks, etc. The frequency and duration of unplanned downtime indicate the reliability and availability of the SaaS vendor, and the potential impact of the service outage on the users' business operations and productivity. References = 3

NEW QUESTION: 237
Which of the following is the MOST effective way for a large and diversified organization to minimize risk associated with unauthorized software on company devices?
A. Scan end points for applications not included in the asset inventory.
B. Prohibit the use of cloud-based virtual desktop software.
C. Conduct frequent reviews of software licenses.
D. Perform frequent internal audits of enterprise IT infrastructure.
Answer: (SHOW ANSWER)
The most effective way for a large and diversified organization to minimize risk associated with unauthorized software on company devices is to scan end points for applications not included in the asset inventory. An asset inventory is a document that records and tracks all the hardware and software assets that are owned,

used, or managed by the organization, such as laptops, tablets, smartphones, servers, applications, etc. An asset inventory helps to identify and classify the assets based on their type, model, location, owner, status, etc.
An asset inventory also helps to monitor and control the assets, such as enforcing security policies, applying patches and updates, detecting and resolving issues, etc. Scanning end points for applications not included in the asset inventory helps to minimize the risk of unauthorized software, because it helps to discover and remove any software that is not approved, authorized, or licensed by the organization, and that may pose security, legal, or operational risks, such as malware, spyware, pirated software, etc. The other options are not as effective as scanning end points for applications not included in the asset inventory, although they may provide some protection or compliance for the software assets. Prohibiting the use of cloud-based virtual desktop software, conducting frequent reviews of software licenses, and performing frequent internal audits of enterprise IT infrastructure are all examples of preventive or detective controls, which may help to prevent or deter the installation or use of unauthorized software, or to verify or validate the software assets, but they do not necessarily discover or remove the unauthorized software. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.1, page 3-11.

NEW QUESTION: 238
The risk associated with an asset before controls are applied can be expressed as:
A. a function of the likelihood and impact
B. the magnitude of an impact
C. a function of the cost and effectiveness of control.
D. the likelihood of a given threat
Answer: A (LEAVE A REPLY)
The risk associated with an asset before controls are applied is also known as the inherent risk. It is the level of risk that exists in the absence of any mitigating actions or measures. To express the inherent risk, one needs to consider two factors: the likelihood and the impact of a potential threat. The likelihood is the probability or frequency of a threat occurring, while the impact is the magnitude or severity of the consequences if the threat materializes. The inherent risk can be calculated by multiplying the likelihood and the impact, or by using a risk matrix that assigns a risk rating based on the combination of these two factors. The other options are not correct ways of expressing the inherent risk, as they do not account for both the likelihood and the impact of a threat. The magnitude of an impact is only one component of the risk, and it does not reflect how likely the threat is to happen. The function of the cost and effectiveness of control is related to the residual risk, which is the risk that remains after controls are applied. The likelihood of a given threat is also only one component of the risk, and it does not indicate how severe the impact would be if the threat occurs. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.1, Page 47.

NEW QUESTION: 239
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?
A. Likelihood of a threat
B. Impact of technology risk

C. Impact of operational risk

D. Control weakness

Answer: (SHOW ANSWER)

A vulnerability report for the IT infrastructure is a document that identifies and evaluates the weaknesses or gaps in the IT systems, networks, or devices that could be exploited by threats or cause incidents. By analyzing the latest vulnerability report, one can conclude the existence and extent of control weaknesses in the IT infrastructure, because control weaknesses are the deficiencies or failures of the controls that are supposed to prevent, detect, or correct the vulnerabilities. The other options are not the correct answers, because they are not directly concluded by analyzing the latest vulnerability report. The likelihood of a threat, the impact of technology risk, and the impact of operational risk are examples of risk factors or consequencesthat depend on the vulnerability and the threat, but they are not determined by the vulnerability report alone. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 240

Which of the following is the FIRST step when developing a business case to drive the adoption of a risk remediation project by senior management?

Freecram.net

A. Calculating the cost

B. Analyzing cost-effectiveness

C. Determining the stakeholders

D. Identifying the objectives

Answer: (SHOW ANSWER)

The first step when developing a business case to drive the adoption of a risk remediation project by senior management is to identify the objectives of the project. The objectives are the specific, measurable, achievable, relevant, and time-bound (SMART) goals that the project aims to accomplish. The objectives should be aligned with the organization's vision, mission, and strategy, as well as the identified business problem or opportunity. The objectives should also reflect the expected benefits and outcomes of the project, such as reducing the risk exposure, enhancing the security posture, or improving the business performance. Identifying the objectives is the first step because it provides the direction, scope, and justification for the project, and it serves as the basis for evaluating the alternative solutions, estimating the costs and benefits, and communicating the value proposition to the senior management and other stakeholders. The other options are not the first step, although they may be subsequent or concurrent steps in the business case development process. Calculating the cost is a part of the financial analysis, which estimates the total expenditure and funding sources of the project, but it does not define the purpose or the scope of the project. Analyzing cost- effectiveness is a part of the economic analysis, which compares the costs and benefits of the alternative solutions and recommends the optimal one, but it does not specify the goals or the criteria of the project.

Determining the stakeholders is a part of the stakeholder analysis, which identifies and assesses the interests, expectations, and influence of the parties involved in or affected by the project, but it does not establish the objectives or the rationale of the project. References = Business case: 7 key steps to build it and use it - Twproject: project ..., Guide to developing the Project Business Case - GOV.UK, How to Write a Business Case: Template & Examples | Adobe Workfront

NEW QUESTION: 241
When should security be considered throughout the development lifecycle of an application?
A. In the design phase.
B. During pre-production testing.
C. Once in the production environment.
D. Throughout development.
Answer: (SHOW ANSWER)
Automated code reviews are most effective when integrated throughout the development lifecycle. Continuous reviews allow early detection and remediation of vulnerabilities, preventing security issues from propagating into later stages such as testing or production. Performing code reviews only at the end or once in production is less effective as vulnerabilities may already be embedded. The proactive approach in development reduces risk significantly

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 242
The PRIMARY reason to implement a formalized risk taxonomy is to:
A. reduce subjectivity in risk management.
B. comply with regulatory requirements.
C. demonstrate best industry practice.
D. improve visibility of overall risk exposure.
Answer: (SHOW ANSWER)
The primary reason to implement a formalized risk taxonomy is to reduce subjectivity in risk management, as it provides a common and consistent language and structure for identifying, classifying, and reporting risks, and facilitates the comparison and aggregation of risks across the organization. The other options are not the primary reasons, as they are more related to the outcomes, benefits, or drivers of risk management, respectively, rather than the reason for risk management. References = CRISC Review Manual, 7th Edition, page 100.

NEW QUESTION: 243
Which of the following would BEST help to address the risk associated with malicious outsiders modifying application data?
A. Multi-factor authentication
B. Role-based access controls

C. Activation of control audits
D. Acceptable use policies
Answer: (SHOW ANSWER)
Role-based access controls (RBAC) are a type of preventive control that limit the access and actions of users based on their roles and responsibilities within the organization. RBAC can help to address the risk of malicious outsiders modifying application data by restricting their access to the data and the functions they can perform on it. RBAC can also enforce the principle of least privilege, which means that users only have the minimum level of access required to perform their tasks. RBAC can be implemented through policies, procedures, and technical mechanisms such as access control lists, encryption, and authentication.
References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1.1, p. 178-179

NEW QUESTION: 244
Which of the following situations reflects residual risk?
A. Risk that is present before risk acceptance has been finalized
B. Risk that is removed after a risk acceptance has been finalized
C. Risk that is present before mitigation controls have been applied
D. Risk that remains after mitigation controls have been applied
Answer: (SHOW ANSWER)
Residual riskrefers to the risk that remains after mitigation measures have been applied. It represents the exposure that an organization decides to accept, transfer, or further address, aligning with its risk appetite and tolerance.

NEW QUESTION: 245
Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?
A. The programming project leader solely reviews test results before approving the transfer to production.
B. Test and production programs are in distinct libraries.
C. Only operations personnel are authorized to access production libraries.
D. A synchronized migration of executable and source code from the test environment to the production environment is allowed.
Answer: (SHOW ANSWER)
The programming project leader solely reviewing test results before approving the transfer to production would be a weakness in procedures for controlling the migration of changes to production libraries, because it violates the principle of segregation of duties, and it exposes the production libraries to the risk of unauthorized or erroneous changes. The programming project leader is responsible for developing and testing the changes, but not for approving and deploying them. The approval and deployment of the changes should be done by an independent and authorized party, such as the change control board or the operations manager.
The other options are not weaknesses, but rather good practices, because:

* Option B: Test and production programs being in distinct libraries is a good practice, because it prevents the accidental or intentional overwriting or mixing of the test and production programs, and it ensures the integrity and security of the production libraries.
* Option C: Only operations personnel being authorized to access production libraries is a good practice, because it restricts the access and modification of the production libraries to the qualified and accountable staff, and it prevents the unauthorized or inappropriate access or modification of the production libraries by other parties.
* Option D: A synchronized migration of executable and source code from the test environment to the production environment being allowed is a good practice, because it ensures the consistency and completeness of the changes, and it avoids the potential errors or discrepancies that may arise from the manual or partial migration of the changes. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 215.

NEW QUESTION: 246
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?
A. Communicate the decision to the risk owner for approval
B. Seek approval from the previous action plan manager.
C. Identify an owner for the new control.
D. Modify the action plan in the risk register.
Answer: (SHOW ANSWER)
A risk mitigation action plan is a document that specifies the actions to be taken to address the identified risks, the resources required, the timelines, the owners, and the expected outcomes. The risk owner is the person who has the authority and accountability to manage the risk and its response. The risk practitioner is the person who supports the risk owner in the risk management process. The best course of action for the risk practitioner when the manager of a risk mitigation action plan is replaced and a new control is implemented is to communicate the decision to the risk owner for approval. This will ensure that the risk owner is aware of the change, agrees with the new control, and approves the modification of the action plan. The other options are not the best course of action, as they may not involve the risk owner, who is ultimately responsible for the risk and its response. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter
3, Section 3.1.1.1, pp. 95-96.

NEW QUESTION: 247
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?
A. A record of incidents is maintained.
B. Forensic investigations are facilitated.
C. Security violations can be identified.
D. Developing threats are detected earlier.
Answer: D (LEAVE A REPLY)

According to the CRISC Review Manual, the greatest benefit of analyzing logs collected from different systems is to detect developing threats earlier, because it helps to identify and correlate the patterns, trends, and anomalies that may indicate a potential attack or compromise. Log analysis is the process of examining and interpreting the log data generated by various systems, such as firewalls, servers, routers, and applications. Log analysis can provide valuable insights into the activities and events that occur on the systems, and can enable the timely detection and response to the emerging threats. The other options are not the greatest benefits of analyzing logs, as they are less proactive or less strategic than detecting developing threats earlier. Maintaining a record of incidents is a benefit of logging, but not of analyzing logs, as it involves storing and preserving the log data for future reference. Facilitating forensic investigations is a benefit of analyzing logs, but it is a reactive and tactical activity that occurs after an incident has happened. Identifying security violations is a benefit of analyzing logs, but it is a specific and operational activity that focuses on the compliance and enforcement of the security policies and standards. References = CRISC Review Manual, 7th Edition, Chapter 5, Section 5.3.2, page 263.

NEW QUESTION: 248
An IT risk practitioner has been tasked to engage key stakeholders to assess risk for key IT risk scenarios. Which of the following is the PRIMARY benefit of this activity?
A. Establishing the available risk mitigation budget
B. Verifying the relevance of risk ratings
C. Demonstrating compliance to regulatory bodies
D. Assessing IT risk management culture
Answer: (SHOW ANSWER)
Stakeholders provide operational insight that enhances the accuracy and context of risk ratings. Their input ensures the ratings reflect actual risk exposure and business priorities, validating the relevance of the assessments.
Reference:CRISC Manual - Domain 2, Slide 256, 404

NEW QUESTION: 249
Which of the following should a risk practitioner review FIRST when evaluating risk events associated with the organization's data flow model?
A. High-level network diagrams
B. Notes from interviews with the data owners
C. Results of data classification activities
D. Recent changes to enterprise architecture (EA)
Answer: (SHOW ANSWER)

NEW QUESTION: 250
An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?
Freecram.net
A. Implement IT systems in alignment with business objectives.
B. Review metrics and key performance indicators (KPIs).

C. Review design documentation of IT systems.
D. Evaluate compliance with legal and regulatory requirements.
Answer: (SHOW ANSWER)
The best way to measure the effectiveness of the subsidiary's IT systems controls is to review metrics and key performance indicators (KPIs), as they provide quantitative and qualitative measures of the performance and outcomes of the IT systems and processes, and how well they meet the predefined standards and expectations. Metrics and KPIs can help to evaluate the efficiency, reliability, security, and quality of the IT systems and controls, and to identify any gaps, weaknesses, or issues that need to be addressed. Metrics and KPIs can also help to compare and benchmark the subsidiary's IT systems and controls with those of the parent organization or other similar entities. The other options are not the best ways to measure the effectiveness of the subsidiary's IT systems controls, although they may be useful or complementary methods.
Implementing IT systems in alignment with business objectives is a good practice, but it does not measure the effectiveness of the IT systems controls, as it focuses on the alignment and integration of the IT systems with the business strategy and goals. Reviewing design documentation of IT systems can provide some information on the specifications and requirements of the IT systems, but it does not measure the effectiveness of the IT systems controls, as it does not reflect the actual implementation and operation of the IT systems. Evaluating compliance with legal and regulatory requirements can ensure that the subsidiary's IT systems and controls meet the minimum standards and obligations of the foreign country, but it does not measure the effectiveness of the IT systems controls, as it does not consider the performance and outcomes of the IT systems and processes. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk and Control Monitoring and Reporting, page 187.

NEW QUESTION: 251
Which of the following is the MOST useful information for prioritizing risk mitigation?
A. Cost of risk mitigation
B. Asset criticality
C. Acceptable risk level
D. Business impact assessment
Answer: (SHOW ANSWER)
Business Impact Assessment (BIA):
* BIA identifies and evaluates the potential effects of interruptions to critical business operations. It helps determine the priority of risk mitigation efforts based on the potential impact on business functions.
* BIA provides detailed information on which processes and systems are most critical to the organization's operations and their respective impact levels.
Prioritizing Risk Mitigation:
* The results of a BIA guide decision-makers in prioritizing which risks to address first based on their potential to disrupt critical business operations.
* Risks that could cause significant operational, financial, or reputational damage are prioritized higher.
Comparing Other Factors:
* Cost of Risk Mitigation: Important but secondary to understanding the impact on business operations.

* Asset Criticality: Relevant but typically part of the BIA process.
* Acceptable Risk Level: Defines the threshold but does not prioritize specific risks.
References:
* The CRISC Review Manual discusses how BIA facilitates risk prioritization by identifying critical processes and their impacts (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.7 Business Impact Analysis).

NEW QUESTION: 252
The MAIN purpose of reviewing a control after implementation is to validate that the control:
A. operates as intended.
B. is being monitored.
C. meets regulatory requirements.
D. operates efficiently.
Answer: A (LEAVE A REPLY)
The main purpose of reviewing a control after implementation is to validate that the control operates as intended, as this can help to ensure that the control is effective and efficient in mitigating the risk, and that it meets the control objectives and requirements. Reviewing a control after implementation can also help to identify and address any issues or gaps that may arise during the control operation, and to monitor and evaluate the performance and impact of the control. Reviewing a control after implementation can also provide feedback and information to the control owners and stakeholders, and enable them to adjust the control design and implementation accordingly. References = Most Asked CRISC Exam Questions and Answers. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 254. ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 254. CRISC by Isaca Actual Free Exam Q&As, Question 9.

NEW QUESTION: 253
The BEST way for an organization to ensure that servers are compliant to security policy is to review:
A. change logs.
B. configuration settings.
C. server access logs.
D. anti-malware compliance.
Answer: (SHOW ANSWER)
Reviewing configuration settings is the best way for an organization to ensure that servers are compliant to security policy, because it helps to check and verify that the servers are configured and maintained according to the established security standards and guidelines, and that any deviations or violations are identified and corrected. A configuration setting is a parameter or option that defines the behavior or functionality of a server, such as a system, an application, or a service. A security policy is a document that outlines the security objectives, principles, and rules that the organization and its employees must follow, and the consequences of non-compliance. Reviewing configuration settings is the best way, as it helps to ensure that the servers are secure and compliant, and that any security risks or issues are detected and resolved. Reviewing change logs, server access logs, and anti-malware compliance are all possible ways to ensure

that servers are compliant to security policy, but they are not the best way, as they do not provide a comprehensive and consistent view of the configuration settings and their compliance status. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.3.2, page 200

NEW QUESTION: 254
An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:
A. mitigation.
B. avoidance.
C. transfer.
D. acceptance.
Answer: (SHOW ANSWER)
Risk transfer is a risk response strategy that involves shifting the responsibility or burden of a risk to another party, such as a third party, an insurance company, or a joint venture. Risk transfer does not eliminate the risk, but it reduces the exposure or impact of the risk to the enterprise. An example of risk transfer is engaging a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. By doing so, the organization transfers the risk of data breach or loss to the third party, who is responsible for ensuring the security and availability of the data. The other options are not examples of risk transfer, as they involve different risk response strategies:
* Risk mitigation is a risk response strategy that involves reducing the likelihood or impact of a risk to an acceptable level, such as by implementing controls, policies, or procedures.
* Risk avoidance is a risk response strategy that involves eliminating the risk by not performing the activity that generates the risk, such as by discontinuing a product or service, or not entering a market.
* Risk acceptance is a risk response strategy that involves acknowledging the risk and taking no action to address it, such as by tolerating the risk, exploiting the risk, or sharing the risk. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3, Section 3.3.1.1, pp. 107-108.

NEW QUESTION: 255
A financial organization is considering a project to implement the use of blockchain technology. To help ensure the organization's management team can make informed decisions on the project, which of the following should the risk practitioner reassess?
A. Business impact analysis (BIA)
B. Risk tolerance
C. Risk classification
D. Risk profile
Answer: (SHOW ANSWER)

NEW QUESTION: 256
Which of the following will be MOST effective in helping to ensure control failures are appropriately managed?
A. Compensating controls

B. Peer review
C. Control ownership
D. Control procedures
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 257
Which of the following will BEST help to ensure implementation of corrective action plans?
A. Contracting to third parties
B. Establishing employee awareness training
C. Setting target dates to complete actions
D. Assigning accountability to risk owners
Answer: (SHOW ANSWER)
Assigning accountability to risk owners is the best way to ensure implementation of corrective action plans, because it clarifies the roles and responsibilities of those who are in charge of managing and mitigating the risks. Contracting to third parties, establishing employee awareness training, and setting target dates to complete actions are all helpful measures, but they do not guarantee the implementation of corrective action plans without accountability. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.3, page 105

NEW QUESTION: 258
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?
A. Risk manager
B. Data owner
C. End user
D. IT department
Answer: (SHOW ANSWER)
The data owner is the person who has the authority and responsibility to classify, label, and protect the information assets of the organization. The data owner is accountable for the risk of potential loss of confidential information, as they are the ones who determine the level of protection and access required for the data. The risk manager is responsible for identifying, assessing, and mitigating the risks that may affect the organization, but they are not accountable for the data itself. The end user is the person who uses the information assets for their operational tasks, but they are not accountable for the data protection or

classification. The IT department is responsible for providing the technical support and infrastructure for the information assets, but they are not accountable for the data ownership or risk management. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.3: Data Classification, p. 69-70.

NEW QUESTION: 259

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

A. To enable consistent data on risk to be obtained

B. To allow for proper review of risk tolerance

C. To identify dependencies for reporting risk

D. To provide consistent and clear terminology

Answer: (SHOW ANSWER)

According to the CRISC Review Manual, the primary objective of providing an aggregated view of IT risk to business management is to enable consistent data on risk to be obtained, because it helps to ensure that the risk information is comparable, reliable, and accurate across the organization. An aggregated view of IT risk is a consolidated and comprehensive representation of the IT risk exposure and impact at the enterprise level, based on the risk identification, analysis, and evaluation processes. Providing an aggregated view of IT risk to business management allows them to understand the overall IT risk profile and performance, and to make informed decisions about the risk management strategies and priorities. The other options are not the primary objective of providing an aggregated view of IT risk, as they are related to other benefits or outcomes of the risk aggregation process. Allowing for proper review of risk tolerance is the objective of establishing the risk context, which defines the scope and boundaries of the risk management activities. Identifying dependencies for reporting risk is the outcome of the risk aggregation process, as it provides a clear and consistent structure and format for the risk communication and reporting. Providing consistent and clear terminology is the objective of developing the risk taxonomy, which is the system of classification and categorization of risks based on common characteristics and attributes. References = CRISC Review Manual, 7th Edition, Chapter 2, Section 2.1.2, page 69.

NEW QUESTION: 260

An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

Freecram.net

A. Lead auditor

B. Project manager

C. Chief audit executive (CAE)

D. Chief information officer (CIO)

Answer: (SHOW ANSWER)

Robotics process automation (RPA) is the use of software robots to perform repetitive, rules-based tasks that interact with multiple applications. RPA can help internal audit departments automate certain continuous

auditing tasks, such as data extraction, validation, analysis, and reporting. RPA can improve the efficiency, quality, and coverage of internal audit activities, and provide greater insight and value to the business. However, RPA also involves certain risks, such as errors, failures, security breaches, or compliance issues, that need to be identified, assessed, and managed. The risk associated with ineffective design of the software bots is the possibility and impact of the bots not functioning as intended, or producing inaccurate or unreliable results. The risk owner of this risk is the person or entity who has the authority and responsibility for managing the risk. The risk owner should be able to define the risk appetite, assess the risk level, select and implement the risk response, monitor and report the risk status, and ensure the risk alignment with the project objectives and strategy. The risk owner of the risk associated with ineffective design of the software bots is the project manager, who is the person in charge of planning, executing, monitoring, and closing the RPA project. The project manager understands the project scope, requirements, budget, timeline, and deliverables, and the potential consequences of ineffective design of the software bots. The project manager also has the resources and incentives to address the risk effectively and efficiently. Therefore, the project manager is the most appropriate risk owner of the risk associated with ineffective design of thesoftware bots. References = Robotic Process Automation for Internal Audit, p. 3-4, Adopting robotic process automation in Internal Audit, Robotic Process Automation (RPA) - Internal Audit Use and Risks.

NEW QUESTION: 261

Which of the following scenarios represents a threat?

A. Connecting a laptop to a free, open, wireless access point (hotspot)

B. Visitors not signing in as per policy

C. Storing corporate data in unencrypted form on a laptop

D. A virus transmitted on a USB thumb drive

Answer: (SHOW ANSWER)

A virus transmitted on a USB thumb drive is a scenario that represents a threat, as it involves a malicious or harmful event that could compromise the confidentiality, integrity, or availability of an information system. A virus is a type of malware that can infect and damage files, programs, or devices by replicating itself and spreading to other systems or networks. A USB thumb drive is a portable storage device that can be used to transfer data between computers or devices. A virus transmitted on a USB thumb drive can occur when a user inserts an infected USB thumb drive into a computer or device, or when a user downloads or copies an infected file from a USB thumb drive to a computer or device. A virus transmitted on a USB thumb drive can pose a serious risk to the information system, as it can corrupt or delete data, disrupt or degrade performance, steal or leak information, or allow unauthorized access or control.

The other options are not scenarios that represent a threat, but rather vulnerabilities or weaknesses that could increase the likelihood or impact of a threat. Connecting a laptop to a free, open, wireless access point (hotspot) is a vulnerability, as it exposes the laptop to potential eavesdropping, interception, or manipulation by malicious actors on the same network. Visitors not signing in as per policy is a vulnerability, as it creates a gap in the physical security and access control of the premises, and could allow unauthorized or malicious visitors to enter or access sensitive areas or assets. Storing corporate data in unencrypted form on a laptop is a vulnerability, as it reduces the protection and security of the data, and could enable unauthorized or malicious access, disclosure, or modification of the data in case of loss, theft, or compromise of the laptop.

References = What is a Computer Virus? | McAfee, What is a USB Flash Drive? | Kingston Technology, Threats, Vulnerabilities, and Exploits - oh my!

NEW QUESTION: 262
Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?
A. IT security manager
B. IT personnel
C. Data custodian
D. Data owner
Answer: (SHOW ANSWER)
The person or entity who should be primarily responsible for performing user entitlement reviews is the data owner. A user entitlement review is a process that verifies and validates the access rights and privileges of the users to the data and resources in the IT environment. A user entitlement review helps to ensure that the users have the appropriate and necessary access to perform their roles and functions, and to prevent or detect any unauthorized or inappropriate access. A data owner is the person or entity that has the authority and responsibility to define, classify, and protect the data and resources in the IT environment. A data owner helps to perform user entitlement reviews, because they help to establish and enforce the access policies and standards for the data and resources, and to approve or revoke the access requests and changes for the users. A data owner also helps to monitor and report on the access performance and compliance for the data and resources, and to identify and address any issues or gaps in the access management activities. The other options are not the primary responsible party for performing user entitlement reviews, although they may be involved in the process. IT security manager, IT personnel, and data custodian are all examples of roles or functions that can help to support or implement the user entitlement reviews, but they do not necessarily have the authority or responsibility to define, classify, or protect the data and resources.
References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.2.1, page 5-14.

NEW QUESTION: 263
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?
A. Third-party software is used for data analytics.
B. Data usage exceeds individual consent.
C. Revenue generated is not disclosed to customers.
D. Use of a data analytics system is not disclosed to customers.
Answer: (SHOW ANSWER)
Data usage exceeding individual consent presents the greatest risk to the organization's reputation, as it violates the privacy and trust of the customers and exposes the organization to legal and regulatory liabilities. Customers have the right to know and control how their personal data is collected, processed, and shared by the organization, and they expect the organization to respect their preferences and comply with the applicable laws and standards. If the organization uses the data for purposes beyond the scope of the consent, or without obtaining the consent in the first place, it may damage its reputation and lose its

customers' loyalty and confidence. Third-party software used for data analytics, revenue generated from data analytics, and use of a data analytics system are not inherently risky to the organization's reputation, as long as they are transparent, secure, and ethical. References = Most Asked CRISC Exam Questions and Answers - The Knowledge Academy; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 203.

NEW QUESTION: 264
An organization wants to grant remote access to a system containing sensitive data to an overseas third party.
Which of the following should be of GREATEST concern to management?
A. Transborder data transfer restrictions
B. Lack of monitoring over vendor activities
C. Differences in regional standards
D. Lack of after-hours incident management support
Answer: (SHOW ANSWER)

NEW QUESTION: 265
A hospital recently implemented a new technology to allow virtual patient appointments. Which of the following should be the risk practitioner's FIRST course of action?
A. Reassess the risk profile.
B. Modify the risk taxonomy.
C. Increase the risk tolerance.
D. Review the risk culture.
Answer: (SHOW ANSWER)
Reassessing the risk profile is the first course of action that a risk practitioner should take after a hospital recently implemented a new technology to allow virtual patient appointments. This is because reassessing the risk profile can help identify, analyze, and evaluate the new or changed risks that the new technology may introduce or affect, such as data privacy, security, quality, reliability, or compliance risks. Reassessing the risk profile can also help determine the appropriate risk response and mitigation strategies, as well as monitor and report the risk performance and outcomes. According to the CRISC Review Manual 2022, reassessing the risk profile is one of the key steps in the IT risk management process1. According to the web search results, reassessing the risk profile is a common and recommended practice for addressing the risks of virtual patient appointments

NEW QUESTION: 266
The PRIMARY objective of the board of directors periodically reviewing the risk profile is to help ensure:
A. the risk strategy is appropriate
B. KRIs and KPIs are aligned
C. performance of controls is adequate
D. the risk monitoring process has been established
Answer: (SHOW ANSWER)

The PRIMARY objective of the board of directors periodically reviewing the risk profile is to help ensure that the risk strategy is appropriate, because the risk strategy defines the enterprise's risk appetite, tolerance, and objectives, and guides the risk management process and activities. The board of directors should review the risk profile to ensure that it reflects the current internal and external environment, and that it aligns with the enterprise's strategy and goals. The other options are not the primary objective, because:
Option B: KRIs and KPIs are aligned is a desirable outcome of the risk strategy, but not the primary objective of the board of directors reviewing the risk profile. KRIs and KPIs are indicators that measure and monitor the risk exposure and performance of the enterprise, respectively, and they should be consistent with the risk strategy and objectives.
Option C: Performance of controls is adequate is a result of the risk response, but not the primary objective of the board of directors reviewing the risk profile. Performance of controls is the degree to which the controls are effective and efficient in mitigating the risks, and it should be evaluated and reported by the risk management function and the internal audit function.
Option D: The risk monitoring process has been established is a prerequisite for the risk profile, but not the primary objective of the board of directors reviewing the risk profile. The risk monitoring process is the process of tracking and reporting the risk status and performance, and it should be implemented and executed by the risk management function and the business process owners. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 119.

NEW QUESTION: 267
Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?
A. Management has not determined a final implementation date.
B. Management has not completed an early mitigation milestone.
C. Management has not secured resources for mitigation activities.
D. Management has not begun the implementation.
Answer: (SHOW ANSWER)
The observation that would be of GREATEST concern to a risk practitioner reviewing the implementation status of management action plans is that management has not begun the implementation, because it indicates that the management action plans are not being executed or monitored, and that the risks are not being addressed or mitigated. The lack of implementation may also imply that the management action plans are not realistic, feasible, or aligned with the enterprise's strategy and objectives. The other options are not as concerning as the lack of implementation, because:
Option A: Management has not determined a final implementation date is a concern, but not the greatest one, because it may affect the timely completion and delivery of the management action plans, but it does not necessarily mean that the management action plans are not being executed or monitored.
Option B: Management has not completed an early mitigation milestone is a concern, but not the greatest one, because it may indicate a delay or deviation in the progress and performance of the management action plans, but it does not necessarily mean that the management action plans are not being executed or monitored.

Option C: Management has not secured resources for mitigation activities is a concern, but not the greatest one, because it may affect the quality and effectiveness of the management actionplans, but it does not necessarily mean that the management action plans are not being executed or monitored. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 123.

NEW QUESTION: 268
Which of the following would BEST help to ensure that identified risk is efficiently managed?
A. Reviewing the maturity of the control environment
B. Regularly monitoring the project plan
C. Maintaining a key risk indicator for each asset in the risk register
D. Periodically reviewing controls per the risk treatment plan
Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), periodically reviewing controls per the risk treatment plan would best help to ensure that identified risk is efficiently managed, as it involves verifying the effectiveness and efficiency of the implemented risk response actions and identifying any gaps or changes in the risk profile. Periodically reviewing controls per the risk treatment plan helps to:
Confirm that the controls are operating as intended and producing the desired outcomes Detect any deviations, errors, or weaknesses in the controls and their performance Evaluate the adequacy and appropriateness of the controls in relation to the current risk environment and the organization's risk appetite and risk tolerance Recommend and implement corrective actions or improvement measures to address any issues or deficiencies in the controls Update the risk register and the risk treatment plan to reflect the current risk status and the residual risk levels References = CRISC Review Manual (Digital Version), Chapter 4: IT Risk Monitoring and Reporting, Section 4.1: IT Risk Monitoring, pp. 215-2161

NEW QUESTION: 269
Which of the following is MOST important to update following a change in organizational risk appetite and tolerance?
A. Business impact assessment (BIA)
B. Key performance indicators (KPIs)
C. Risk profile
D. Industry benchmark analysis
Answer: (SHOW ANSWER)
The risk profile is the most important document to update following a change in organizational risk appetite and tolerance, because it summarizes the current and target state of the organization's risk exposure, as well as the risk response strategies and actions. The risk profile should reflect the alignment of the organization's risk appetite and tolerance with its strategic objectives and operational capabilities. Updating the risk profile will help the organization to monitor and manage its risks effectively and efficiently.
References
*ISACA CRISC Review Manual, 7th Edition, Domain 1: IT Risk Identification, Section 1.2.1: Risk Profile
*Risk Profile - ISACA
*What is a Risk Profile? Definition, Examples, and More

NEW QUESTION: 270

Which of the following is the BEST method to identify unnecessary controls?

A. Evaluating the impact of removing existing controls

B. Evaluating existing controls against audit requirements

C. Reviewing system functionalities associated with business processes

D. Monitoring existing key risk indicators (KRIs)

Answer: (SHOW ANSWER)

The best method to identify unnecessary controls is reviewing system functionalities associated with business processes, because this can help to determine whether the controls are relevant, effective, and efficient for the current business needs and objectives. System functionalities are the capabilities and features of IT systems that support the execution and performance of business processes. Business processes are the set of interrelated activities that transform inputs into outputs to deliver value to customers or stakeholders. By reviewing system functionalities associated with business processes, an organization can assess whether the controls are aligned with the process requirements, expectations, and outcomes, and whether they add value or create waste. The review can also identify any gaps, overlaps, redundancies, or conflicts among the controls, and any changes or improvements that are needed to optimize the controls. The other options are less effective methods to identify unnecessary controls. Evaluating the impact of removing existing controls can help to measure the benefits and costs of the controls, but it does not address the root causes or sources of the unnecessary controls. Evaluating existing controls against audit requirements can help to ensure compliance and assurance, but it does not consider the business context or purpose of the controls. Monitoring existing key risk indicators (KRIs) can help to measure the level and impact of risks, but it does not evaluate the suitability or adequacy of the controls. References = Surveying Staff to Identify Unnecessary Internal Controls - Methodology and Results

NEW QUESTION: 271

A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

A. Obtain the risk owner's approval.

B. Record the risk as accepted in the risk register.

C. Inform senior management.

D. update the risk response plan.

Answer: (SHOW ANSWER)

A compensating control is a temporary or alternative control that is implemented when the primary control for mitigating a risk is not feasible or available. A compensating control should provide a similar level of protection and assurance as the primary control, and should be aligned with the risk appetite and tolerance of the organization. The risk practitioner's best course of action when a compensating control needs to be applied is to obtain the risk owner's approval. The risk owner is the person who has the authority and accountability for managing a specific risk, and who is responsible for ensuring that the risk is within the acceptable level. The risk practitioner should consult with the risk owner to explain the situation, proposethe compensating control, and seek their approval before implementing it. This way, the risk practitioner can

ensure that the compensating control is appropriate, effective, and acceptable for the risk owner, and that the risk owner is aware of and agrees with the change in the risk treatment. The other options are not the best course of action, as they do not involve the risk owner's approval or input. Recording the risk as accepted in the risk register implies that the risk is not treated or reduced, which may not be the case with a compensating control. Informing senior management may be a good practice, but it does not ensure that the risk owner is involved or agrees with the compensating control. Updating the risk response plan may be a necessary step after implementing the compensating control, but it does not require the risk owner's approval or consultation. References = 5 Key Risk Mitigation Strategies (With Examples), Risk Management 101: Process, Examples, Strategies

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 272
Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?
A. Continuous monitoring
B. A control self-assessment
C. Transaction logging
D. Benchmarking against peers
Answer: (SHOW ANSWER)
* Events exceeding risk thresholds are situations or occurrences that result in the actual level of risk exceeding the acceptable or tolerable level of risk, as defined by the organization's risk appetite, criteria, and objectives12.
* The most effective way to enable a business operations manager to identify events exceeding risk thresholds is to implement continuous monitoring, which is a process that involves collecting and analyzing data and information on the performance and status of the business processes, systems, and controls, and detecting and reporting any deviations, anomalies, or issues that may indicate a risk event34.
* Continuous monitoring is the most effective way because it provides timely and accurate visibility and insight into the risk landscape, and enables the business operations manager to identify and respond to the events exceeding risk thresholds before they escalate or cause significant harm or damage to the organization34.
* Continuous monitoring is also the most effective way because it supports the risk management process and objectives, which are to identify and address the risks that may affect the achievement of the organization's goals and the delivery of value to the stakeholders34.

* The other options are not the most effective ways, but rather possible tools or techniques that may complement or enhance the continuous monitoring. For example:
* A control self-assessment is a technique that involves engaging and empowering the business process owners and operators to evaluate and report on the effectiveness and efficiency of the controls that are designed and implemented to mitigate the risks56. However, this technique is not the most effective way because it is periodic rather than continuous, and it may not capture or communicate the events exceeding risk thresholds in a timely or consistent manner56.
* Transaction logging is a tool that involves recording and storing the details and history of the transactions or activities that are performed by the business processes or systems, and providing an audit trail for verification or investigation purposes78. However, this tool is not the most effective way because it is passive rather than active, and it may not detect or report the events exceeding risk thresholds unless they are analyzed or queried78.
* Benchmarking against peers is a technique that involves comparing and contrasting the performance and practices of the business processes or systems with those of the similar or leading organizations in the same or related industry, and identifying the gaps or opportunities for improvement . However, this technique is not the most effective way because it is external rather than internal, and it may not reflect or align with the organization's specific risk appetite, criteria, and objectives . References =
* 1: Risk IT Framework, ISACA, 2009
* 2: IT Risk Management Framework, University of Toronto, 2017
* 3: Continuous Monitoring - ISACA1
* 4: Continuous Monitoring: A New Approach to Risk Management - ISACA Journal2
* 5: Risk and control self-assessment - KPMG Global3
* 6: Control Self Assessments - PwC4
* 7: Transaction Log - Wikipedia5
* 8: Transaction Logging - IBM6
* : Benchmarking - Wikipedia7
* : Benchmarking: Definition, Types, Process, Advantages & Examples

NEW QUESTION: 273
What is the PRIMARY benefit of risk monitoring?
A. It reduces the number of audit findings.
B. It provides statistical evidence of control efficiency.
C. It facilitates risk-aware decision making.
D. It facilitates communication of threat levels.
Answer: (SHOW ANSWER)
Risk monitoring is the process of tracking and evaluating the performance and effectiveness of the risk management process and controls, and identifying any changes or emerging risks that may affect the enterprise's objectives and strategy. The primary benefit of risk monitoring is that it facilitates risk-aware decision making, as it provides timely and relevant information and feedback to the decision-makers and stakeholders, and enables them to adjust the risk strategy and response actions accordingly. Risk monitoring also helps to ensure that the risk management process is aligned with the enterprise's risk appetite and

tolerance, and supports the achievement of the enterprise's goals and value creation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 239. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 239. CRISC Sample Questions 2024, Question 239.

NEW QUESTION: 274

Which of the following is the BEST key performance indicator (KPI) to measure the maturity of an organization's security incident handling process?

A. The number of security incidents escalated to senior management

B. The number of resolved security incidents

C. The number of newly identified security incidents

D. The number of recurring security incidents

Answer: (SHOW ANSWER)

A security incident handling process is a set of procedures and activities that aim to identify, analyze, contain, eradicate, recover from, and learn from security incidents that affect the confidentiality, integrity, or availability of information assets12.

The maturity of a security incident handling process is the degree to which the process is defined, managed, measured, controlled, and improved, and the extent to which it meets the organization's objectives and expectations34.

The best key performance indicator (KPI) to measure the maturity of a security incident handling process is the number of recurring security incidents, which is the frequency or rate of security incidents that are repeated or reoccur after being resolved or closed56.

The number of recurring security incidents is the best KPI because it reflects the effectiveness and efficiency of the security incident handling process, and the ability of the process to prevent or reduce the recurrence of security incidents through root cause analysis, corrective actions, and continuous improvement56.

The number of recurring security incidents is also the best KPI because it is directly related to the organization's objectives and expectations, such as minimizing the impact and cost of security incidents, enhancing the security posture and resilience of the organization, and complying with the relevant standards and regulations56.

The other options are not the best KPIs, but rather possible metrics that may support or complement the measurement of the maturity of the security incident handling process. For example:

The number of security incidents escalated to senior management is a metric that indicates the severity or complexity of security incidents, and the involvement or awareness of the seniormanagement in the security incident handling process56. However, this metric doesnot measure the effectiveness or efficiency of the process, or the ability of the process to prevent or reduce security incidents56.

The number of resolved security incidents is a metric that indicates the output or outcome of the security incident handling process, and the performance or productivity of the security incident handling team56. However, this metric does not measure the quality or sustainability of the resolution, or the ability of the process to prevent or reduce security incidents56.

The number of newly identified security incidents is a metric that indicates the input or demand of the security incident handling process, and the capability or capacity of the security incident detection and identification

mechanisms56. However, this metric does not measure the effectiveness or efficiency of the process, or the ability of the process to prevent or reduce security incidents56. References =
1: Computer Security Incident Handling Guide, NIST Special Publication 800-61, Revision 2, August 2012
2: ISO/IEC 27035:2016 Information technology - Security techniques - Information security incident management
3: Capability Maturity Model Integration (CMMI) for Services, Version 1.3, November 2010
4: COBIT 2019 Framework: Introduction and Methodology, ISACA, 2018
5: KPIs for Security Operations & Incident Response, SecurityScorecard Blog, June 7, 2021
6: Key Performance Indicators (KPIs) for Security Operations and Incident Response, DFLabs White Paper, 2018

NEW QUESTION: 275
The maturity of an IT risk management program is MOST influenced by:
A. the organization's risk culture
B. benchmarking results against similar organizations
C. industry-specific regulatory requirements
D. expertise available within the IT department
Answer: (SHOW ANSWER)
The maturity of an IT risk management program is most influenced by the organization's risk culture, as this reflects the shared values, beliefs, and attitudes that shape how the organization perceives and responds to risk. The risk culture determines the level of awareness, commitment, and involvement of the stakeholders in the IT risk management process, as well as the degree of integration and alignment with the enterprise's objectives and strategy. A mature IT risk management program requires a strong and positive risk culture that fosters trust, collaboration, and accountability among the stakeholders, and supports continuous improvement and learning. The other options are not the most influential factors for the maturity of an IT risk management program, although they may have some impact or relevance. Benchmarking results against similar organizations can provide useful insights and comparisons, but they do not necessarily reflect the organization' s own risk culture or context. Industry-specific regulatory requirements can impose certain standards and expectations, but they do not guarantee the effectiveness or efficiency of the IT risk management program.
Expertise available within the IT department can enhance the technical and operational aspects of the IT risk management program, but it does not ensure the strategic and cultural alignment with the enterprise.
References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, page 23.

NEW QUESTION: 276
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?
A. Enroll the employee in additional security training.
B. Invoke the incident response plan.
C. Conduct an internal audit.

D. Instruct the vendor to delete the data.

Answer: (SHOW ANSWER)

The best recommendation for a risk practitioner upon learning that an employee inadvertently disclosed sensitive data to a vendor is to invoke the incident response plan. An incident responseplan is a document that defines the roles, responsibilities, procedures, and resources fordetecting, analyzing, containing, eradicating, recovering, and reporting on security incidents that could affect the organization's IT systems or data. An incident response plan helps to protect and restore the confidentiality, integrity, and availability of the organization's information assets, and to comply with the relevant laws, regulations, standards, and contracts.

Invoking the incident response plan is the best recommendation, because it helps to respond to and mitigate the security incident, and to minimize the damage and impact of the data disclosure. Invoking the incident response plan also helps to communicate and coordinate the incident response actions and strategies with the internal and external stakeholders, such as the data owners, users, custodians, and regulators, and to report and disclose the incident as required. The other options are not as effective as invoking the incident response plan, although they may be part of or derived from the incident response plan. Enrolling the employee in additional security training, conducting an internal audit, and instructing the vendor to delete the data are all examples of corrective or preventive actions, which may help to prevent or deter the recurrence of the data disclosure, or to verify or validate the data security, but they do not necessarily address or resolve the current security incident. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.4.1, page 5-
32.

NEW QUESTION: 277

Who is PRIMARILY accountable for risk treatment decisions?

A. Risk owner

B. Business manager

C. Data owner

D. Risk manager

Answer: (SHOW ANSWER)

The risk owner is primarily accountable for risk treatment decisions, as they are the person or entity with the authority and responsibility to manage a particular risk. The risk owner should evaluate the available risk response options, select the most appropriate one, implement the chosen response, and monitor its effectiveness. The risk owner should also communicate and report on the risk status and any issues or changes. The business manager, data owner, and risk manager are not primarily accountable for risk treatment decisions, although they may be involved in the risk management process. The business manager is responsible for the overall performance and objectives of a business unit or function. The data owner is responsible for the security and quality of a specific data asset. The risk manager is responsible for facilitating and coordinating the risk management activities across the organization. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 47.

NEW QUESTION: 278

Who should be accountable for ensuring effective cybersecurity controls are established?
A. Risk owner
B. Security management function
C. IT management
D. Enterprise risk function
Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), the security management function is responsible for ensuring that effective cybersecurity controls are established and maintained. The security management function should:
Define the cybersecurity strategy and objectives aligned with the enterprise's risk appetite and business goals Establish and maintain the cybersecurity policies, standards, procedures and guidelines Implement and monitor the cybersecurity controls and processes Coordinate and communicate with other stakeholders, such as risk owners, IT management, enterprise risk function, internal and external auditors, regulators and third parties Report on the cybersecurity performance and risk posture to senior management and the board Continuously improve the cybersecurity capabilities and maturity References = CRISC Review Manual (Digital Version), Chapter 1: IT Risk Identification, Section 1.4: IT Risk Management Roles and Responsibilities, pp. 29-301

NEW QUESTION: 279
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?
A. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test
B. Percentage of issues arising from the disaster recovery test resolved on time
C. Percentage of IT systems included in the disaster recovery test scope
D. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test
Answer: (SHOW ANSWER)
The most important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes is the percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test. The RTO is the maximum acceptable time that a system orprocess can be unavailable after a disruption. The disaster recovery test is a simulation of a disaster scenario to evaluate the readiness and capability of the organization to restore its critical functions and systems. By measuring the percentage ofIT systems meeting the RTO during the test, the organization can assess how well the disaster recovery processes meet the predefined objectives and standards. Percentage of IT systems recovered within the mean time to restore (MTTR), percentage of issues arising from the disaster recovery test resolved on time, and percentage of IT systems included in the disaster recovery test scope are other possible KPIs, but they are not as important as the percentage of IT systems meeting the RTO. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 12; CRISC Review Manual, 6th Edition, page 215.

NEW QUESTION: 280

An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

Freecram.net

A. Initiate a retest of the full control

B. Retest the control using the new application as the only sample.

C. Review the corresponding change control documentation

D. Re-evaluate the control during (he next assessment

Answer: (SHOW ANSWER)

The best course of action when a new application is added to the environment after testing of the SSO control has been completed is to initiate a retest of the full control, as it may reveal any new issues or gaps that the new application may introduce to the SSO control, and ensure that the control remains effective and adequate.

Retesting the control using the new application as the only sample, reviewing the corresponding change control documentation, and re-evaluating the control during the next assessment are not the best courses of action, as they may not provide sufficient assurance, evidence, or timeliness of the control testing, respectively. References = CRISC Review Manual, 7th Edition, page 154.

NEW QUESTION: 281

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?

A. Number of users that participated in the DRP testing

B. Number of issues identified during DRP testing

C. Percentage of applications that met the RTO during DRP testing

D. Percentage of issues resolved as a result of DRP testing

Answer: (SHOW ANSWER)

A key performance indicator (KPI) is a measurable value that demonstrates how effectively an organization is achieving its objectives. In the context of disaster recovery planning (DRP), a KPI should reflect the ability of the organization to recover its critical business processes and applications within the predefined time frames and service levels. One of the most important KPIs for DRP is the percentage of applications that met the recovery time objective (RTO) during DRP testing. The RTO is the maximum acceptable length of time that a business process or application can be down after a disaster. By measuring the percentage of applications that met the RTO during DRP testing, the organization can evaluate the performance and reliability of its DRP, identify any gaps or weaknesses, and implement corrective actions to improve its readiness and resilience.

The other options are not the best KPIs for DRP, as they do not directly measure the effectiveness of the recovery process. The number of users that participated in the DRP testing is a measure of the involvement and awareness of the staff, but not of the outcome of the testing. The number of issues identified during DRP testing is a measure of the quality and completeness of the DRP, but not of the actual recovery time. The percentage of issues resolved as a result of DRP testing is a measure of the improvement and maturity of the DRP, but not of the current recovery capability. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3, Section 3.2.3.3, Page 138.

NEW QUESTION: 282
Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?
A. Risk owner
B. Risk practitioner
C. Compliance manager
D. Control owner
Answer: (SHOW ANSWER)
The risk practitioner is responsible for determining which stakeholders need to be involved in the development of a risk scenario, as they have the knowledge and skills to facilitate the process and ensure that the relevant perspectives and information are considered. The risk owner, the compliance manager, and the control owner are examples of stakeholders who may participate in the risk scenario development, but they are not responsible for determining who should be involved. References = Risk Scenarios Toolkit, page 9; CRISC Review Manual, 7th Edition, page 101.

NEW QUESTION: 283
Which of the following is a KEY responsibility of the second line of defense?
A. Implementing control activities
B. Monitoring control effectiveness
C. Conducting control self-assessments
D. Owning risk scenarios
Answer: (SHOW ANSWER)
The second line of defense is a group of functions that provide oversight, guidance, and monitoring of the risk management activities of the first line of defense. The second line of defense includes risk management, compliance, and internal control departments. Their key responsibility is to monitor the effectiveness of the control activities implemented by the first line of defense, and to report any issues or gaps to senior management and the board. The second line of defense also supports the first line of defense by providing frameworks, policies, tools,and techniques to identify, measure, and manage risks. The other options are not the key responsibility of the second line of defense, as explained below:
A: Implementing control activities is the responsibility of the first line of defense, which consists of the business units and process owners that own and manage the risks associated with their daily operations.
C: Conducting control self-assessments is a technique used by the first line of defense to evaluate the design and operation of their own controls, and to identify and report any deficiencies or improvement opportunities.
D: Owning risk scenarios is the responsibility of the first line of defense, which is accountable for the risks inherent in their business activities, and for developing and executing risk response strategies. References = Modernizing The Three Lines of Defense Model | Deloitte US, The second line of defence: fit for purpose, not an uncomfortable fit | Knowledge | Linklaters, COSO's Take on the Three Lines of Defense | ERM - Enterprise Risk Management, Three Lines of Defense | Risk Management - Schneider Downs CPAs, What is the Three Lines of Defense Approach to Risk Management?

NEW QUESTION: 284
Which of the following is MOST important for managing ethical risk?
A. Involving senior management in resolving ethical disputes
B. Developing metrics to trend reported ethics violations
C. Identifying the ethical concerns of each stakeholder
D. Establishing a code of conduct for employee behavior
Answer: D (LEAVE A REPLY)
Establishing a code of conduct for employee behavior is the most important factor for managing ethical risk, because it defines the standards and expectations for ethical conduct and decision making within the organization, and provides guidance and direction for employees to act in a responsible and ethical manner. Ethical risk is the risk of violating the moral principles or values that govern the behavior and actions of individuals or organizations, such as honesty, integrity, fairness, or respect. A code of conduct is a document that outlines the ethical principles, values, and rules that the organization and its employees must follow, and the consequences of non-compliance. A code of conduct helps to promote a positive and ethical culture within the organization, and to prevent or mitigate the ethical risks that may arise from conflicts of interest, fraud, corruption, discrimination, or other misconduct. Involving senior management in resolving ethical disputes, developing metrics to trend reported ethics violations, and identifying the ethical concerns of each stakeholder are all useful factors for managing ethical risk, but they are not the most important factor, as they do not directly address the ethical conduct and decision making of employees. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.5.1, page 67

NEW QUESTION: 285
When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?
A. Mapping threats to organizational objectives
B. Reviewing past audits
C. Analyzing key risk indicators (KRIs)
D. Identifying potential sources of risk
Answer: (SHOW ANSWER)
Identifying potential sources of risk is the first step in the risk identification process, which is essential for developing a thorough understanding of risk scenarios. Sources of risk can be internal or external, and can include factors such as people, processes, technology, environment, regulations, and events. Identifying potential sources of risk can help to generate a comprehensive list of risk scenarios that can affect the organization's objectives and operations. Identifying potential sources of risk can also help to raise risk awareness among the employees and to foster a risk culture within the organization. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.1, p. 66-67

NEW QUESTION: 286
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?
A. Risk management strategy planning

B. Risk monitoring and control
C. Risk identification
D. Risk response planning
Answer: (SHOW ANSWER)
* A risk register is a document that records and tracks the information about the risks that may affect the organization's objectives, such as the risk description, category, source, cause, impact, probability, status, owner, response, etc.
* When developing a new risk register, a risk practitioner should focus on risk identification. This is the process of finding, recognizing, and describing the risks that may affect the organization's objectives, using various techniques, such as brainstorming, interviews, checklists, surveys, etc.
* Risk identification helps to create a comprehensive and accurate list of the risks that need to be managed, and to provide the basis for the subsequent risk analysis and evaluation, risk response planning, and risk monitoring and control.
* The other options are not the risk management activities that a risk practitioner should focus on when developing a new risk register. They are either subsequent or parallel to risk identification.
The references for this answer are:
* Risk IT Framework, page 29
* Information Technology & Security, page 23
* Risk Scenarios Starter Pack, page 21

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 287
During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?
A. Business process owners
B. Business process consumers
C. Application architecture team
D. Internal audit
Answer: (SHOW ANSWER)
The MOST important stakeholders to include during the initial risk identification process for a business application are the business process owners, because they are the ones who have the authority and responsibility for the business processes that are supported or enabled by the business application. The business process owners can provide valuable input and feedback on the business objectives, requirements, and expectations of the business application, as well as thepotential risks, impacts, and opportunities that

may affect the business processes and outcomes. The other options are not as important as the business process owners, because:
Option B: Business process consumers are the ones who use or benefit from the business processes that are supported or enabled by the business application, such as customers, employees, or partners. They can provide useful information and perspectives on the user needs, preferences, and satisfaction of the business application, but they are not as important as the business process owners, who have the ultimate accountability and authority for the business processes and outcomes.
Option C: Application architecture team is the one who designs and develops the technical architecture and components of the business application, such as the hardware, software, network, and data. They can provide technical expertise and guidance on the feasibility, functionality, and security of the business application, but they are not as important as the business process owners, who have the primary stake and interest in the business application and its alignment with the business processes and objectives.
Option D: Internal audit is the one who provides independent assurance and consulting services on the governance, risk management, and control processes of the organization, including the business application. They can provide objective and impartial evaluation and recommendation on the effectiveness and efficiency of the business application and its compliance with the internal and external standards and regulations, but they are not as important as the businessprocess owners, who have the direct involvement and influence on the business application and its performance and value. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 103.

NEW QUESTION: 288
Deviation from a mitigation action plan's completion date should be determined by which of the following?
A. Change management as determined by a change control board
B. Benchmarking analysis with similar completed projects
C. Project governance criteria as determined by the project office
D. The risk owner as determined by risk management processes
Answer: D (LEAVE A REPLY)
Deviation from a mitigation action plan's completion date should be determined by the risk owner as determined by risk management processes, because the risk owner is the person or entity who has the accountability and authority to manage the risk and its associated mitigation actions. The risk owner should monitor and report the progress and status of the mitigation action plan, and determine if there is any deviation from the expected completion date, based on the risk management processes and criteria. The other options are not the ones who should determine the deviation, because:
Option A: Change management as determined by a change control board is a process that ensures that any changes to the project scope, schedule, cost, or quality are controlled and approved, but it does not determine the deviation from the mitigation action plan's completion date, which is a risk management activity.
Option B: Benchmarking analysis with similar completed projects is a technique that compares the performance and practices of the current project with those of similar or successful projects, but it does not determine the deviation from the mitigation action plan's completion date, which is a risk management activity.

Option C: Project governance criteria as determined by the project office is a set of rules and standards that define the roles, responsibilities, and authority of the project stakeholders, but it does notdetermine the deviation from the mitigation action plan's completion date, which is a risk management activity. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p.
122.

NEW QUESTION: 289
Which of the following BEST balances the costs and benefits of managing IT risk*?
A. Prioritizing and addressing risk in line with risk appetite. Eliminating risk through preventive and detective controls
B. Considering risk that can be shared with a third party
C. Evaluating the probability and impact of risk scenarios
Answer: (SHOW ANSWER)
Risk appetite is the broad-based amount of risk that an organization is willing to accept in its activities. Risk appetite reflects the level of risk that the organization is prepared to take to achieve its strategic goals, and provides guidance and boundaries for the risk management activities and decisions. The best way to balance the costs and benefits of managing IT risk is to prioritize and address risk in line with risk appetite, which means that the organization should identify, assess, treat, monitor, and communicate the risks that are within or exceed the risk appetite, and allocate the resources and efforts accordingly. By doing so, the organization can optimize its risk-return trade-off, align its risk exposure with its strategic objectives, and enhance its risk culture and performance. References = 5

NEW QUESTION: 290
Which of the following statements in an organization's current risk profile report is cause for further action by senior management?
Freecram.net
A. Key performance indicator (KPI) trend data is incomplete.
B. New key risk indicators (KRIs) have been established.
C. Key performance indicators (KPIs) are outside of targets.
D. Key risk indicators (KRIs) are lagging.
Answer: (SHOW ANSWER)
A risk profile report is a document that summarizes the current status and trends of the risks that an organization faces, as well as the actions taken or planned to manage them1. A risk profile report is a useful tool for senior management to monitor and oversee the organization's risk management performance and to make informed decisions and adjustments as needed2. One of the key components of a risk profile report is the key performance indicators (KPIs), which are metrics used to measure and evaluate the achievement of the organization's objectives and strategies3. KPIs are aligned with the organization's risk appetite and tolerance, and they have specific targets or benchmarks that indicate the desired level of performance4. Therefore, if the KPIs are outside of targets, it means that the organization is not meeting its objectives and strategies, and that there may be gaps or issues in the risk management process or the risk response actions. This is a cause for further action by senior management, as they need to investigate the root causes of the deviation, assess the impact and implications of the underperformance, and take corrective or

preventive measures to improve the situation and bring the KPIs back to the targets. Incomplete KPI trend data, new KRIs, and lagging KRIs are not the most critical statements in a risk profile report that require further action by senior management, as they do not directly indicate a failure or a problem in the risk management performance or the achievement of the objectives and strategies. Incomplete KPI trend data means that there is missing or insufficient information on the historical or projected changes in the KPIs over time. This may affect the accuracy and reliability of the risk profile report, but it does not necessarily mean that the KPIs are outside of targets or that the objectives and strategies are not met. Senior management may need to request or obtain the complete KPI trend data, but this is not as urgent or important as addressing the KPIs that are outside of targets. New KRIs means that there are additional or revised metrics used to measure and monitor the level of risk associated with a particular process, activity, or system within the organization. This may reflect the changes or updates in the risk environment, the risk appetite and tolerance, or the risk assessment methodology. However, new KRIs do not directly indicate a failure or a problem in the risk management performance or the achievement of the objectives and strategies. Senior management may need to review and approve the new KRIs, but this is not as urgent or important as addressing the KPIs that are outside of targets. Lagging KRIs means that there are metrics that measure and monitor the level of risk after a risk event has occurred or a risk response has been implemented. This may provide useful feedback and lessons learned for the risk management process, but it does not directly indicate a failure or a problem in the risk management performance or the achievement of the objectives and strategies. Senior management may need to analyze and evaluate the lagging KRIs, but this is not as urgent or important as addressing the KPIs that are outside of targets. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section
4.3: Risk Reporting, pp. 201-205.

NEW QUESTION: 291
Which of the following provides the MOST helpful information in identifying risk in an organization?
A. Risk registers
B. Risk analysis
C. Risk scenarios
D. Risk responses
Answer: (SHOW ANSWER)
Risk scenarios provide the MOST helpful information in identifying risk in an organization, because they describe the possible events, causes, effects, and impacts of a risk on the organization's objectives and processes. Risk scenarios help to identify the sources, drivers, and indicators of risk, as well as the potential consequences and likelihood of occurrence. The other options are not as helpful as risk scenarios, because:
Option A: Risk registers are tools to document and track the identified risks, their characteristics, and their status, but they do not provide information on how to identify risks in the first place.
Option B: Risk analysis is a process to assess the likelihood and impact of the identified risks, and to prioritize them based on their severity, but it does not provide information on how to identify risks in the first place.

Option D: Risk responses are actions to address the identified risks, either by reducing, transferring, avoiding, or accepting them, but they do not provide information on how to identify risks in the first place. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 105.

NEW QUESTION: 292
A public online information security training course is available to an organization's staff. The online course contains free-form discussion fields. Which of the following should be of MOST concern to the organization's risk practitioner?
A. The form may be susceptible to SQL injection attacks.
B. Data is not encrypted in transit to the site.
C. Proprietary corporate information may be disclosed.
D. Staff nondisclosure agreements (NDAs) are not in place.
Answer: (SHOW ANSWER)
Free-form fields in public forums increase the risk of accidental or intentional disclosure of sensitive or proprietary information. This creates legal and reputational exposure. Monitoring or disabling such features is essential to mitigating data leakage risks.
Reference:CRISC Manual - Domain 2, Slide 124-127, 203

NEW QUESTION: 293
A review of an organization s controls has determined its data loss prevention {DLP) system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?
A. Key risk indicators (KRIs)
B. Inherent risk
C. Residual risk
D. Risk appetite
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after applying controls to mitigate the inherent risk. Inherent risk is the risk that exists before considering the controls. Key risk indicators (KRIs) are metrics that measure the level and impact of risks. Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. The failure of the data loss prevention (DLP) system to detect outgoing emails containing credit card data would most impact the residual risk, because it would increase the likelihood and impact of data leakage, data loss, and data exfiltration incidents. These incidents could cause financial, reputational, legal, and regulatory damages to the organization. The failure of the DLP system would also affect the KRIs, as they would show a higher level of risk exposure and a lower level of control effectiveness. However, the KRIs are not the risk itself, but rather the indicators of the risk. The failure of the DLP system would not directly impact the inherent risk or the risk appetite, as they are independent of the controls. The inherent risk would remain the same, as it is based on the nature and value of the data and the threats and vulnerabilities that exist. The risk appetite would also remain the same, as it is based on the organization's culture, strategy, and stakeholder expectations. Therefore, the most impacted factor would be the residual

risk, as it reflects the actual risk level that the organization faces after applying the controls. References = Risk IT Framework, ISACA, 2022, p. 131

NEW QUESTION: 294
Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?
A. Approval by senior management
B. Low cost of development and maintenance
C. Sensitivity to changes in risk levels
D. Use of industry risk data sources
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics that help organizations monitor and assess potential risks that may impact their operations, financial health, or overall performance1. KRIs should have certain characteristics that make them effective for risk monitoring, such as:
Ability to measure the right thing (e.g., supports the decisions that need to be made) Quantifiable (e.g., damages in dollars of profit loss) Capability to be measured precisely and accurately Relevant (measuring the right thing associated with decisions)2 Among the four options given, only option C (sensitivity to changes in risk levels) best enables effective risk monitoring. This is because KRIs should be able to capture the changes in risk levels over time and alert organizations to emerging or escalating risks3. A high sensitivity to changes in risk levels indicates that theKRI is responsive and timely, and can help organizations take preventive or corrective actions before the risks become too severe.
References = Key Risk Indicators: A Practical Guide, Key Risk Indicators: Examples & Definitions, Key Risk Indicators - Wikipedia

NEW QUESTION: 295
An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?
A. More time has been allotted for testing.
B. The project is likely to deliver the product late.
C. A new project manager is handling the project.
D. The cost of the project will exceed the allotted budget.
Answer: (SHOW ANSWER)
Being the first to market is a competitive advantage that can help an organization gain market share, customer loyalty, and brand recognition. However, this advantage can be lost if the project is delayed and the competitors catch up or surpass the organization. Therefore, the project delivery time is of greatest concern to senior management, as it directly affects the strategic objective of the project. The other options are less critical, as they can be managed or mitigated by the project team. More time for testing can improve the quality and reliability of the product, a new project manager can bring fresh ideas and perspectives, and the cost overrun can be justified by the expected benefits and revenues of the product. References = Project Initiation: The First Step to Project Management [2023] * Asana, 12 Steps to Initiate and Plan a Successful Project

NEW QUESTION: 296
Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?
A. Insurance coverage
B. Security awareness training
C. Policies and standards
D. Risk appetite and tolerance
Answer: (SHOW ANSWER)
Policies and standards are the primary documents that define the organization's expectations and requirements for information security and risk management. They provide the basis for establishing controls, procedures, roles, and responsibilities. Policies and standards should be updated following a change in legislation requiring notification to individuals impacted by data breaches, to ensure compliance with the new legal obligations and to align with the organization's risk appetite and tolerance. Updating policies and standards can also help to communicate the changes to the relevant stakeholders and to provide guidance for implementing and monitoring the controls. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.2, p. 28-29

NEW QUESTION: 297
Which of the following controls will BEST detect unauthorized modification of data by a database administrator?
A. Reviewing database access rights
B. Reviewing database activity logs
C. Comparing data to input records
D. Reviewing changes to edit checks
Answer: (SHOW ANSWER)
Unauthorized modification of data by a database administrator is a security risk that involves altering, deleting, or inserting data on a database without proper authorization or approval, by a person who has privileged access to the database, such as a database administrator12.
The best control to detect unauthorized modification of data by a database administrator is to review database activity logs, which are records that capture and store the details and history of the transactions or activities that are performed on the database, such as who, what, when, where, and how34.
Reviewing database activity logs is the best control because it provides evidence and visibility of the database operations, and enables the detection and reporting of any deviations, anomalies, or issues that may indicate unauthorized modification of data by a database administrator34.
Reviewing database activity logs is also the best control because it supports the accountability and auditability of the database operations, and facilitates the investigation and resolution of any unauthorized modification of data by a database administrator34.
The other options are not the best controls, but rather possible measures or techniques that may supplement or enhance the review of database activity logs. For example:

Reviewing database access rights is a measure that involves verifying and validating the permissions and privileges that are granted or revoked to the users or roles who can access or modify the data on the database56. However, this measure is not the best control because it does not directly detect unauthorized modification of data by a database administrator, especially if the database administrator has legitimate access rights to the data56.
Comparing data to input records is a technique that involves matching and reconciling the data on the database with the original or source data that are entered or imported into the database, and identifying and correcting any discrepancies or errors78. However, this technique is not the best control because it does not directly detect unauthorized modification of data by a database administrator, especially if the input records are also modified or compromised78.
Reviewing changes to edit checks is a technique that involves examining and evaluating the modifications or updates to the edit checks, which are rules or validations that are applied to the data on the database to ensure their accuracy, completeness, andconsistency9 . However, this technique is not the best control because it does not directly detect unauthorized modification of data by a database administrator, especially if the edit checks are bypassed or disabled9 . References =
1: Database Security: Attacks and Solutions | SpringerLink2
2: Unauthorised Modification of Data With Intent to Cause Impairment3
3: Database Activity Monitoring - Wikipedia4
4: Database Activity Monitoring (DAM) | Imperva5
5: Database Access Control - Wikipedia6
6: Database Access Control: Best Practices for Database Security7
7: Data Reconciliation - Wikipedia8
8: Data Reconciliation and Gross Error Detection9
9: Edit Check - Wikipedia
Edit Checks: A Data Quality Tool

NEW QUESTION: 298
A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?
A. Periodic user privileges review
B. Log monitoring
C. Periodic internal audits
D. Segregation of duties
Answer: (SHOW ANSWER)
The best control to help reduce the risk of fraudulent internal transactions in several business applications is the segregation of duties. Segregation of duties is the principle of dividing the roles and responsibilities of different individuals or groups involved in a business process or an IT service, so that no one person or group has complete control over the entire process or service. Segregation of duties can help to prevent or detect fraud, errors, conflicts of interest, or misuse of resources, by ensuring that there are checks and balances, and that there is adequate oversight and accountability. Segregation of duties can also help to reduce the risk of collusion, compromise, or coercion among the internal staff, by limiting their access and

authority to the business applications and data. Periodic user privileges review, log monitoring, and periodic internal audits are also useful controls, but they are not as effective as segregation of duties, as they are reactive and detective measures, rather than proactive and preventive measures. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 299
A control owner identifies that the organization's shared drive contains personally identifiable information (PII) that can be accessed by all personnel. Which of the following is the MOST effective risk response?
A. Protect sensitive information with access controls.
B. Implement a data loss prevention (DLP) solution.
C. Re-communicate the data protection policy.
D. Implement a data encryption solution.
Answer: (SHOW ANSWER)
Personally identifiable information (PII) is any information that can be used to identify, contact, or locate an individual, such as name, address, phone number, email, social security number, etc1. PII is subject to various laws and regulations that aim to protect the privacy and security of individuals' data1. Organizations that collect, store, process, or transmit PII have a responsibility to safeguard it from unauthorized access, use, disclosure, modification, or destruction1.
One of the best practices for protecting PII is to implement access controls, which are mechanisms that restrict access to PII based on the principle of least privilege2. Access controls ensure that only authorized personnel who have a legitimate need to access PII can do so, and that they can only perform the actions that are necessary for their roles and responsibilities2. Access controls can be implemented at different levels, such as network, system, application, or data level, and can use various methods, such as passwords, tokens, biometrics, encryption, etc2.
If an organization's shared drive contains PII that can be accessed by all personnel, this poses a high risk of data breach, theft, loss, or misuse, which could result in legal, financial, reputational, or operational consequences for the organization and the individuals whose data is compromised3. Therefore, the most effective risk response is to protect the sensitive information with access controls, such as:
* Classify the PII according to its sensitivity and impact level, and assign appropriate labels and permissions to the data files and folders2.
* Restrict access to the shared drive to only those personnel who have a valid business reason to access the PII, and grant them the minimum level of access required to perform their tasks2.
* Implement strong authentication and authorization mechanisms, such as multifactor authentication, role-based access control, or attribute-based access control, to verify the identity and privileges of the users who access the shared drive2.
* Encrypt the PII stored on the shared drive, and use secure protocols and channels to transmit the data over the network2.
* Monitor and audit the access and activities on the shared drive, and generate logs and reports to detect and respond to any unauthorized or anomalous events2.
The other options are not as effective as access controls, because they do not directly address the root cause of the risk, which is the lack of access restrictions on the shared drive. Implementing a data loss

prevention (DLP) solution, which is a tool that monitors and prevents the leakage of sensitive data, may help to detect and block some unauthorized data transfers, but it does not prevent unauthorized access or viewing of the PII on the shared drive4. Re-communicating the data protection policy, which is a document that defines the rules and responsibilities for handling PII, may help to raise awareness and compliance among the personnel, but it does not enforce or verify the actual implementation of the policy. Implementing a data encryption solution, which is a technique that transforms the PII into an unreadable format, may help to protect the confidentiality of the data, but it does not prevent unauthorized access or modification of the data, and it may introduce additional complexity and overhead to the data management process.
References = Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Best Practices for Protecting PII, How to Secure Personally Identifiable Information against Loss or Compromise, Data Loss Prevention (DLP) | Microsoft 365 security, [Protecting Personal Information: A Guide for Business], [Encryption - Wikipedia]

NEW QUESTION: 300

A risk practitioner has been notified of a social engineering attack using artificial intelligence (AI) technology to impersonate senior management personnel. Which of the following would BEST mitigate the impact of such attacks?

Freecram.net

A. Subscription to data breach monitoring sites
B. Suspension and takedown of malicious domains or accounts
C. Increased monitoring of executive accounts
D. Training and awareness of employees for increased vigilance
Answer: (SHOW ANSWER)
Training employees to recognize and respond to social engineering tactics is the most effective way to mitigate these attacks. It empowers staff to act as the first line of defense, aligning withRisk Awareness and Organizational Trainingpractices.

NEW QUESTION: 301
Which of the following is the MOST important success factor when introducing risk management in an organization?
A. Implementing a risk register
B. Defining a risk mitigation strategy and plan
C. Assigning risk ownership
D. Establishing executive management support
Answer: (SHOW ANSWER)
Establishing executive management support is the most important success factor when introducing risk management in an organization. This is because executive management support can help ensure that risk management is aligned with the organization's vision, mission, and strategy, as well as provide the necessary resources, authority, and accountability for risk management activities. Executive management support can also help foster a risk-aware culture, promote stakeholder engagement, and facilitate risk communication and reporting. According to the CRISC Review Manual 2022, one of the key elements of IT governance is to obtain executive management support and commitment for risk management1. According

to the web search results, executive management support is a critical success factor for risk management in various contexts and industries234.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 302
Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?
A. Relevant risk case studies
B. Internal audit findings
C. Risk assessment results
D. Penetration testing results
Answer: (SHOW ANSWER)
The most helpful factor for an information security management team when allocating resources to mitigate exposures is the risk assessment results. The risk assessment results provide a comprehensive and objective analysis of the risks facing the enterprise, including their likelihood, impact, and root causes. The risk assessment results also help to identify the gaps and weaknesses in the existing controls, and to prioritize the risks based on their severity and urgency. The risk assessment results enable the information security management team to allocate the resources in a cost-effective and risk-based manner, and to implement the most appropriate risk responses to reduce the exposures to an acceptable level. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.1.1, page 1751

NEW QUESTION: 303
The PRIMARY benefit of classifying information assets is that it helps to:
A. communicate risk to senior management
B. assign risk ownership
C. facilitate internal audit
D. determine the appropriate level of control
Answer: (SHOW ANSWER)
* Classifying information assets is a process of identifying and categorizing the data and information resources that are owned, controlled, or used by an organization, based on their value, sensitivity, and criticality.
* Classifying information assets helps to determine the appropriate level of control that is needed to protect them from unauthorized access, use, disclosure, modification, or destruction. Control level refers to the degree of protection or assurance that a control provides against a risk.

* Classifying information assets also helps to communicate risk to senior management, assign risk ownership, and facilitate internal audit. These are other benefits of risk management that are not directly related to determining the appropriate level of control.
The references for this answer are:
* Risk IT Framework, page 11
* Information Technology & Security, page 5
* Risk Scenarios Starter Pack, page 3

NEW QUESTION: 304
IT disaster recovery point objectives (RPOs) should be based on the:
A. maximum tolerable downtime.
B. maximum tolerable loss of data.
C. need of each business unit.
D. type of business.
Answer: (SHOW ANSWER)
IT disaster recovery point objectives (RPOs) should be based on the:
B: maximum tolerable loss of data.
RPOs are determined by how much data loss an organization can withstand in the event of a disaster. It's a measure of the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. Therefore, RPOs are directly related to the maximum tolerable loss of data.

NEW QUESTION: 305
An organization has outsourced its customer management database to an external service provider. Of the following, who should be accountable for ensuring customer data privacy?
A. The vendor's risk manager
B. The organization's information security manager
C. The organization's business process owner
D. The organization's vendor management officer
Answer: (SHOW ANSWER)

NEW QUESTION: 306
An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?
A. Feedback from end users
B. Results of a benchmark analysis
C. Recommendations from internal audit
D. Prioritization from business owners
Answer: (SHOW ANSWER)

A benchmark analysis is a process of comparing the organization's performance, practices, and processes with those of other organizations in the same industry or sector. A benchmark analysis can provide the most useful information when determining the frequency of risk assessments, because it can help the organization to identify the best practices, standards, and expectations for security risk management in its industry. A benchmark analysis can also help the organization to assess its current level of maturity, capability, and compliance in relation to security risk management, and to determine the gaps and areas for improvement. By conducting a benchmark analysis, the organization can establish a realistic and appropriate frequency of risk assessments that aligns with its industry norms and its own risk profile. The other options are not as useful as a benchmark analysis, because they do not provide a comprehensive and relevant view of the security risk management landscape, but rather focus on specific or partial aspects of the organization's situation. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.2, page 18.

NEW QUESTION: 307
Which of the following is the BEST approach for selecting controls to minimize risk?
A. Industry best practice review
B. Risk assessment
C. Cost-benefit analysis
D. Control-effectiveness evaluation
Answer: (SHOW ANSWER)
The best approach for selecting controls to minimize risk is to perform a risk assessment. A risk assessment is a process that identifies, analyzes, and evaluates the risks that could affect the organization's objectives or operations. A risk assessment helps to determine the likelihood and impact of the risks, and to prioritize them based on their severity and relevance. A risk assessment also helps to select the most appropriate and effective controls to minimize the risks, such as avoiding, reducing, transferring, or accepting the risks. A risk assessment is the best approach for selecting controls, because it helps to align the controls with the organization's risk profile, risk appetite, and risk objectives, and to ensure that the controls are adequate, suitable, and cost-effective. The other options are not the best approach for selecting controls, although they may be part of or derived from the risk assessment. Industry best practice review, cost-benefit analysis, and control-effectiveness evaluation are all activities that can help to support or improve the control selection, but they are not the best approach for selecting controls. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 308
Which of the following will BEST help in communicating strategic risk priorities?
A. Heat map
B. Business impact analysis (BIA)
C. Balanced Scorecard
D. Risk register
Answer: (SHOW ANSWER)

The best tool for communicating strategic risk priorities is a heat map. A heat map is a graphical representation of the risk profile of an enterprise, showing the likelihood and impact of various risks on a matrix. A heat map can help to highlight the most significant risks that require attention, as well as the risk appetite and tolerance levels of the enterprise. A heat map can also facilitate the comparison of risks across different business units, processes, or objectives, and enable the communication of risk information to stakeholders in a clear and concise manner. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.3.1, page 240.

NEW QUESTION: 309
When an organization faces potential risks due to changes in data protection legislation in foreign jurisdictions, what is the most appropriate course of action?
A. Ensure compliance with local legislation because it has a higher priority.
B. Conduct a risk assessment and develop mitigation options.
C. Terminate the current cloud contract and migrate to a local cloud provider.
D. Accept the risk because foreign legislation does not apply to the organization.
Answer: (SHOW ANSWER)
When regulatory conflicts arise, the best practice is to conduct a comprehensive risk assessment to understand the impact and develop appropriate mitigation strategies. Immediate termination may be premature without understanding options, and accepting risk without assessment may expose the organization to legal or compliance issues. Prioritizing compliance requires understanding the full scope of risks and controls necessary#5:35, 5:48 CRISC_SentenceinNOTE30.pptx#.

NEW QUESTION: 310
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired.
What is the BEST course of action for this team member?
Freecram.net
A. Enforce segregation of duties.
B. Disclose potential conflicts of interest.
C. Delegate responsibilities involving the acquaintance.
D. Notify the subsidiary's legal team.
Answer: (SHOW ANSWER)
A conflict of interest is a situation where a person's personal or professional interests may interfere with their ability to act in the best interest of the organization or the project1. A conflict of interest can compromise the integrity, objectivity, and impartiality of the person, and create ethical or legal issues for the organization or the project2. In the context of due diligence, a conflict of interest can affect the quality and reliability of the information and analysis, and jeopardize the success and confidentiality of the acquisition3.
The best course of action for a member of the due diligence team who realizes a close acquaintance is a high- ranking IT professional at a subsidiary of the company about to be acquired is to disclose potential conflicts of interest. This means that the team member should inform the due diligence leader and the organization's management about the relationship with the acquaintance, and explain how it may affect their

role or responsibility in the due diligence process. By disclosing potential conflicts of interest, the team member can:
Demonstrate honesty and transparency, and uphold the ethical standards and values of the organization and the project4.
Enable the due diligence leader and the organization's management to assess the situation and decide the appropriate course of action, such as reassigning the team member, implementing additional controls or safeguards, or obtaining consent or approval from the relevant parties5.
Avoid or minimize the negative consequences or risks that may arise from the conflict of interest, such as legal liability, reputational damage, or loss of trust and credibility6.
References =
Conflict of Interest - CIO Wiki
What is a Conflict of Interest? Give Me Some Examples - The Balance Careers How to Avoid Conflicts of Interest in M&A Transactions - DealRoom How to Handle Conflicts of Interest - Harvard Business Review Conflict of Interest Policy - ISACA Managing Conflicts of Interest in the Public Sector Toolkit - OECD

NEW QUESTION: 311
Which of the following is MOST important to review when evaluating the ongoing effectiveness of the IT risk register?
A. The costs associated with mitigation options
B. The status of identified risk scenarios
C. The cost-benefit analysis of each risk response
D. The timeframes for risk response actions
Answer: (SHOW ANSWER)
The status of identified risk scenarios, because it helps to monitor and track the current level and direction of the IT risks, and to determine whether the risk responses and controls are adequate and effective. An IT risk register is a document that records and tracks the key IT risks that an organization faces, along with their likelihood, impact, and response strategies. An IT risk scenario is a hypothetical situation or event that describes the source, cause, consequence, and impact of an IT risk. The status of identified risk scenarios is the most important factor, as it reflects the actual and potential outcomes of the IT risks, and the performance and progress of the risk management process. The costs associated with mitigation options, the cost-benefit analysis of each risk response, and the timeframes for risk response actions are all possible factors to review when evaluating the ongoing effectiveness of the IT risk register, but they are not the most important factor, as they do not directly measure and report the status of the IT risk scenarios.

NEW QUESTION: 312
Which of the following is the BEST recommendation of a risk practitioner for an organization that recently changed its organizational structure?
A. Communicate the new risk profile.
B. Implement a new risk assessment process.
C. Revalidate the corporate risk appetite.
D. Review and adjust key risk indicators (KRIs).

Answer: (SHOW ANSWER)

Communicating the new risk profile is the best recommendation for a risk practitioner for an organization that recently changed its organizational structure, because it helps to inform and align the stakeholders on the current state of risks and their implications for the organization's objectives and strategy. A risk profile is a summary of the key risks that an organization faces, along with their likelihood, impact, and response strategies. An organizational structure is the way that an organization arranges its people, roles, and responsibilities to achieve its goals and deliver its value proposition. A change in the organizational structure may affect the risk profile, as it may introduce new sources or types of risk, or alter the existing risk levels or responses. Therefore, communicating the new risk profile is the best recommendation, as it helps to ensure that the stakeholders are aware of and prepared for the changes and challenges that the new organizational structure may bring. Implementing a new risk assessment process, revalidating the corporate risk appetite, and reviewing and adjusting key risk indicators (KRIs) are all important tasks to perform after communicating the new risk profile, but they are not the best recommendation, as they depend on the communication and understanding of the new risk profile. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.3, page 91

NEW QUESTION: 313

A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

A. The user requirements were not documented.

B. Payroll files were not under the control of a librarian.

C. The programmer had access to the production programs.

D. The programmer did not involve the user in testing.

Answer: (SHOW ANSWER)

A payroll manager discovers that fields in certain payroll reports have been modified without authorization. This indicates that there is a risk of unauthorized access, use, disclosure, modification, or destruction of sensitive data, such as employee information, payroll records, tax returns, etc.

A control weakness that could have contributed most to this problem is that the programmer had access to the production programs. This means that the programmer could potentially alter the source code or configuration of the payroll software without proper authorization or approval.

The other options are not control weaknesses that could have contributed most to this problem. They are either irrelevant or less likely to cause unauthorized changes in the payroll software.

The references for this answer are:

Risk IT Framework, page 12

Information Technology & Security, page 6

Risk Scenarios Starter Pack, page 4

NEW QUESTION: 314

Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

A. Insurance coverage

B. Onsite replacement availability
C. Maintenance procedures
D. Installation manuals
Answer: (SHOW ANSWER)
The MOST important consideration when performing a risk assessment of a fire suppression system within a data center is the maintenance procedures, because they ensure that the fire suppression system is functioning properly and reliably, and that it can prevent or minimize the damage caused by fire incidents. The maintenance procedures should include regular testing, inspection, and servicing of the fire suppression system components, such as sprinklers, detectors, alarms, and extinguishers. The other options are not as important as the maintenance procedures, because:
Option A: Insurance coverage is a financial measure that can compensate for the loss or damage caused by fire incidents, but it does not prevent or reduce the likelihood or impact of the fire incidents. Insurance coverage is also dependent on the terms and conditions of the insurance policy, which may not cover all the scenarios or costs of the fire incidents.
Option B: Onsite replacement availability is a contingency measure that can facilitate the recovery or restoration of the fire suppression system after a fire incident, but it does not prevent or reduce the likelihood or impact of the fire incidents. Onsite replacement availability is alsodependent on the availability and compatibility of the replacement parts, which may not match the original fire suppression system specifications or requirements.
Option D: Installation manuals are a reference source that can provide guidance on how to install or configure the fire suppression system, but they do not ensure that the fire suppression system is functioning properly and reliably. Installation manuals are also static documents that may not reflect the current or updated fire suppression system standards or practices. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 211.

NEW QUESTION: 315
Which of the following is the MOST effective way to validate organizational awareness of cybersecurity risk?
A. Conducting security awareness training
B. Updating the information security policy
C. Implementing mock phishing exercises
D. Requiring two-factor authentication
Answer: (SHOW ANSWER)
Implementing mock phishing exercises is the most effective way to validate organizational awareness of cybersecurity risk, because it helps to measure and test the knowledge and behavior of the employees regarding the detection and prevention of phishing attacks, which are one of the most common and dangerous forms of cybersecurity risk. A phishing attack is a fraudulent attempt to obtain sensitive or confidential information, such as usernames, passwords, or credit card details, by impersonating a legitimate or trusted entity, such as a bank, a government agency, or a colleague, through email, phone, or other communication channels. A mock phishing exercise is a simulated phishing attack that is conducted by the organization or a third party to assess the level of awareness and readiness of the employees to recognize and respond to phishing attacks, and to provide feedback and training to improve their skills and knowledge.

Implementing mock phishing exercises is the most effective way, as it helps to validate the actual and practical awareness of cybersecurity risk, and to identify and address the gaps or weaknesses in the employees' awareness and behavior. Conducting security awareness training, updating the information security policy, and requiring two-factor authentication are all useful ways to enhance organizational awareness of cybersecurity risk, but they are not the most effective way, as they do not directly validate the awareness and behavior of the employees regarding phishing attacks. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

NEW QUESTION: 316
Which of the following is BEST measured by key control indicators (KCIs)?
A. Historical trends of the organizational risk profile
B. Cost efficiency of risk treatment plan projects
C. Comprehensiveness of risk assessment procedures
D. Effectiveness of organizational defense in depth
Answer: (SHOW ANSWER)
Key control indicators are designed to measure the operational effectiveness of controls, specifically their contribution to defense-in-depth strategies. This helps assess if controls are functioning as intended to mitigate identified risks, aligning with Control Effectiveness Monitoring.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 317
Which of the following methods would BEST contribute to identifying obscure risk scenarios?
A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis
Answer: A (LEAVE A REPLY)
Brainstorming sessions would best contribute to identifying obscure risk scenarios, as they allow participants to generate and share ideas without being constrained by conventional thinking or assumptions. Brainstorming sessions can help to identify risks that are not obvious, not well understood, or not covered by existing controls. Control self-assessments, vulnerability analysis, and Monte Carlo analysis are useful methods for evaluating and quantifying risks, but they are not designed to identify obscure risk scenarios. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 59.

NEW QUESTION: 318
An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?
A. Conduct a risk analysis.
B. Initiate a remote data wipe.
C. Invoke the incident response plan
D. Disable the user account.
Answer: (SHOW ANSWER)
The best recommendation for a risk practitioner when an employee lost a personal mobile device that may contain sensitive corporate information is to initiate a remote data wipe. A remote data wipe is a process of erasing the data stored on a device remotely, using a command sent over anetwork or a wireless connection. A remote data wipe can help to prevent the unauthorized access, use, disclosure, or theft of the sensitive corporate information, and to minimize the potential impact of the loss on the enterprise's reputation, operations, and compliance. A remote data wipe can also help to comply with the data breach notification laws and regulations, and to reduce the legal liability and penalties. Conducting a risk analysis, invoking the incident response plan, and disabling the user account are not as immediate and effective as initiating a remote data wipe, as they do not address the primary risk of data exposure and loss. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 319
A failure in an organization's IT system build process has resulted in several computers on the network missing the corporate endpoint detection and response (EDR) software. Which of the following should be the risk practitioner's IMMEDIATE concern?
A. Threats are not being detected.
B. Multiple corporate build images exist.
C. The IT build process was not followed.
D. The process documentation was not updated.
Answer: (SHOW ANSWER)
The primary concern is the immediate risk of undetected threats due to missing endpoint protection. Addressing this ensures the organization's ability to detect and respond to security incidents, aligning withIncident Detection and Responseprinciples.

NEW QUESTION: 320
It is MOST important to the effectiveness of an IT risk management function that the associated processes are:
Freecram.net
A. aligned to an industry-accepted framework.
B. reviewed and approved by senior management.
C. periodically assessed against regulatory requirements.
D. updated and monitored on a continuous basis.
Answer: D (LEAVE A REPLY)

The effectiveness of an IT risk management function depends on how well it can identify, analyze, evaluate, and treat the IT-related risks that may affect the organization's objectives and performance. To achieve this, the IT risk management function needs to have processes that are updated and monitored on a continuous basis, so that they can capture the changes in the IT environment, the business context, the risk appetite and tolerance, and the regulatory requirements. Updating and monitoring the IT risk management processes also helps to ensure that they are consistent, reliable, and efficient, and that they provide timely and accurate information for decision making and reporting12. Aligning the IT risk management processes to an industry-accepted framework is important, but not the most important factor for the effectiveness of the function. A framework provides a common language, structure, and methodology for IT risk management, but it does not guarantee that the processes are updated and monitored on a continuous basis. A framework also needs to be customized and adapted to the specific needs and context of the organization3. Reviewing and approving the IT risk management processes by senior management is important, but not the most important factor for the effectiveness of the function. Senior management support and endorsement are essential for establishing the tone and culture of IT risk management, as well as for allocating the necessary resources and authority for the function. However, senior management review and approval alone do not ensure that the processes are updated and monitored on a continuous basis. Senior management also need to oversee and evaluate the performance and outcomes of the IT risk management function4. Periodically assessing the IT risk management processes against regulatory requirements is important, but not the most important factor for the effectiveness of the function. Regulatory compliance is one of the objectives and drivers of IT risk management, and it requires the function to adhere to the applicable laws, rules, and standards. However, regulatory requirements are not the only source of IT risk, and they may not cover all the aspects and dimensions of IT risk management. Moreover, periodic assessment may not be sufficient to capture the dynamic and evolving nature of IT risk. Therefore, the IT risk management processes need to be updated and monitored on a continuous basis, not only to meet the regulatory requirements, but also to address the other sources and impacts of IT risk5. References = Risk and Information Systems Control Study Manual, Chapter
3: IT Risk Response, Section 3.1: Risk Response Process, pp. 121-123.

NEW QUESTION: 321
To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:
A. risk mitigation approach
B. cost-benefit analysis.
C. risk assessment results.
D. vulnerability assessment results
Answer: (SHOW ANSWER)
To help ensure all applicable risk scenarios are incorporated into the risk register, it is most important to review the risk assessment results, which are the outputs of the process of identifying, analyzing, and evaluating the risks that affect a project or an organization. The risk assessment results provide information on the sources, causes, impacts, likelihood, and severity of the risks, as well as the existing controls and their effectiveness. The risk assessment results help to determine the risk level and priority of each risk

scenario, and to select the most appropriate risk response strategy. The risk assessment results are the basis for creating and updating the risk register, which is a document that records and tracks the identified risks, their characteristics, responses, owners, and status12. The other options are not the most important factors to review, as they are either derived from or dependent on the risk assessment results. The risk mitigation approach is the plan and actions to reduce the impact or likelihood of the risks, and it is based on the risk assessment results. The cost-benefit analysis is the comparison of the costs and benefits of implementing the risk response strategy, and it is influenced by the risk assessment results. The vulnerability assessment results are the identification and measurement of the weaknesses or gaps in the information systems or resources, and they are part of the risk assessment results. References = Risk Assessment in Project Management | PMI; Risk Assessment Process: Definition, Steps, and Examples; Risk Assessment - an overview | ScienceDirect Topics; Risk Register: A Project Manager's Guide with Examples [2023] * Asana; What Is a Risk Register? | Smartsheet

NEW QUESTION: 322
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?
A. KRI thresholds
B. Integrity of the source data
C. Control environment
D. Stakeholder requirements
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics used by organizations to monitor and assess potential risks that may impact their objectives and performance. KRIs also provide early warning signals that help organizations identify, analyze, and address risks before they escalate into significant issues1. The most important factor to understand when developing KRIs is stakeholder requirements, which are the needs and expectations of the persons or entities that have an interest or influence in the organization's risk management2. By understanding stakeholder requirements, the organization can ensure that the KRIs are aligned with the organization's strategy, vision, and mission, and that they reflect the current and emerging risks and their potential consequences. Understanding stakeholder requirements can also help to establish and communicate the roles and responsibilities of the stakeholders, and to enforce the accountability and performance of the risk management. KRI thresholds, integrity of the source data, and control environment are not the most important factors to understand when developing KRIs, as they do not provide the same level of insight and relevance as stakeholder requirements. KRI thresholds are the values or ranges that indicate the level of risk exposure and the need for action or escalation3. KRI thresholds can help to measure and monitor the performance and compliance of the risk management, but they do not ensure that the KRIs are appropriate and accurate for the organization's risk profile. Integrity of the source data is the quality and reliability of the data that are used to support or enable the development of KRIs4. Integrity of the source data can enhance the validity and consistency of the KRIs, but it does not ensure that the KRIs are comprehensive and compatible with the organization's risk environment. Control environment is the set of policies, processes, and systems that provide the foundation and structure for the risk management5. Control environment can improve the security and efficiency of the risk management, but it does not ensure that the KRIs are relevant and realistic for the organization's risk objectives and strategies. References = 1: Key Risk

Indicators: A Practical Guide | SafetyCulture2: Stakeholder Requirements - an overview | ScienceDirect Topics3: Risk Threshold:
Definition, Meaning & Example - PM Study Circle4: Data Integrity - an overview | ScienceDirect Topics5: Control Environment - an overview | ScienceDirect Topics : [Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.1: Key Risk Indicators, pp. 181-185.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.1: Control Design, pp. 233-235.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.2: Control Implementation, pp. 243-245.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.3: Control Monitoring and Maintenance, pp. 251-253.]

NEW QUESTION: 323
Which of the following will BEST help an organization evaluate the control environment of several third- party vendors?
A. Review vendors' internal risk assessments covering key risk and controls.
B. Obtain independent control reports from high-risk vendors.
C. Review vendors performance metrics on quality and delivery of processes.
D. Obtain vendor references from third parties.
Answer: (SHOW ANSWER)
An organization may rely on third-party vendors to provide some of its IT systems, applications, or services, such as cloud computing, software development, or data processing. The organization should evaluate the control environment of the third-party vendors, which is the set of policies, procedures, and practices that establish the tone and culture of the vendor's risk management and control activities. The best way to evaluate the control environment of several third-party vendors is to obtain independent control reports from high-risk vendors. Independent control reports are the documents that attest to the design, implementation, and effectiveness of the vendor's controls, based on the standards or frameworks that are relevant and applicable for the vendor's services, such as the ISAE 3402 or the SOC 2. Independent control reports are prepared by independent and qualified auditors, who provide an objective and reliable assessment of the vendor's controls.
High-risk vendors are the vendors that pose the highest level of risk to the organization, such as by having access to sensitive or confidential data, or by providing critical or complex services. By obtaining independent control reports from high-risk vendors, the organization can verify that the vendor's controls are adequate and appropriate for the organization's needs, and that the vendor complies with thecontractual and regulatory requirements. The other options are not as good as obtaining independent control reports from high-risk vendors, as they may not provide sufficient or consistent information or evidence on the vendor's control environment:
Review vendors' internal risk assessments covering key risk and controls means that the organization examines the vendor's own evaluation of its risks and controls, such as by reviewing the vendor's risk register, risk matrix, or risk report. This may provide some information or insight on the vendor's control environment, but it may not be as reliable or objective as obtaining independent control reports, as the

vendor' s internal risk assessments may have biases, conflicts, or gaps in their methodology, scope, or quality.
Review vendors performance metrics on quality and delivery of processes means that the organization measures and monitors the vendor's performance and outcomes, such as by using key performance indicators (KPIs), service level agreements (SLAs), or customer satisfaction surveys. This may provide some information or feedback on the vendor's control environment, but it may not be as comprehensive or relevant as obtaining independent control reports, as the vendor's performance metrics may not cover all the aspects or components of the vendor's controls, or may not reflect the latest or updated status or results of the vendor's controls.
Obtain vendor references from third parties means that the organization collects and verifies the testimonials or recommendations of the vendor's services from other customers or stakeholders, such as by contacting them directly or by reading their reviews or ratings. This may provide some information or evidence on the vendor's control environment, but it may not be as accurate or consistent as obtaining independent control reports, as the vendor's references from third parties may have biases, conflicts, or variations in their expectations, experiences, or opinions of the vendor's services. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.1.2.1, pp. 147-148.

NEW QUESTION: 324
Winch of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project He cycle?
A. Number of projects going live without a security review
B. Number of employees completing project-specific security training
C. Number of security projects started in core departments
D. Number of security-related status reports submitted by project managers
Answer: A (LEAVE A REPLY)
The number of projects going live without a security review is the best key control indicator (KCI) to indicate whether security requirements are identified and managed throughout a project life cycle, because it measures the compliance and effectiveness of the security review process. A security review is a process that ensures that the security requirements are defined, implemented, tested, and verified for each project, and that any security risks or issues are identified and resolved before the project is deployed. The number of projects going live without a security review should be minimized or eliminated, as it indicates a failure or weakness of the security review process. The other options are not the best KCIs, because they do not directly measure the identification and management of security requirements. The number of employees completing project-specific security training, the number of security projects started in core departments, and the number of security-related status reports submitted by project managers are examples of input or output indicators that measure the activities or results of the project, but not the security requirements. References = CRISC:
Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 325
Which of the following is the PRIMARY reason for managing emerging risk?

A. Assumptions about the future state are likely to become invalid.
B. The organization is likely to become prone to continuous disruptive events.
C. Risk assessment methodologies cannot be applied to emerging risk.
D. The number of risk scenarios may become uncontrollably high.
Answer: (SHOW ANSWER)

NEW QUESTION: 326
The BEST reason to classify IT assets during a risk assessment is to determine the:
A. priority in the risk register.
B. business process owner.
C. enterprise risk profile.
D. appropriate level of protection.
Answer: (SHOW ANSWER)
Classifying IT assets during a risk assessment is a process of assigning values to the IT assets based on their importance, sensitivity, and criticality to the enterprise. The best reason to classify IT assets is to determine the appropriate level of protection that each IT asset requires, based on its value and the potential impact of its loss or compromise. This helps the enterprise to allocate resources and implement controls that are proportional to the risk exposure of the IT assets, and to optimize the cost and benefit of risk mitigation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 233. CRISC by Isaca Actual Free Exam Q&As, Question 9. CRISC Sample Questions 2024, Question 233. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 233.

NEW QUESTION: 327
What is the MOST important consideration when selecting key performance indicators (KPIs) for control monitoring?
A. Source information is acquired at stable cost.
B. Source information is tailored by removing outliers.
C. Source information is readily quantifiable.
D. Source information is consistently available.
Answer: (SHOW ANSWER)
The most important consideration when selecting KPIs for control monitoring is that the source information is consistently available, meaning that it can be obtained regularly, reliably, and timely from the same or equivalent data sources. This ensures that the KPIs can measure the performance of the controls over time and across different units or functions, and provide meaningful and comparable results. Source information that is acquired at stable cost, tailored by removing outliers, or readily quantifiable are also desirable, but not as essential as consistency.
References:
*ISACA, Risk IT Framework, 2nd Edition, 2019, p. 751
*ISACA, Performance Measurement Metrics for IT Governance2

NEW QUESTION: 328
Which of the following is the BEST evidence of a well-defined risk event?
A. Forensic investigations include chain-of-custody requirements
B. Impact analyses include annual loss expectancy (ALE)
C. Incident response plans include recovery time objectives (RTOs)
D. Critical systems include key performance indicators (KPIs)
Answer: (SHOW ANSWER)
Annual Loss Expectancy (ALE) quantifies a risk event's expected financial impact and is derived from Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO).
CRISC guidance states:
"A well-defined risk event includes quantified impact analysis such as annual loss expectancy to facilitate prioritization and comparison." Chain-of-custody and KPIs are unrelated to defining risk events.
Hence, B is correct.
CRISC Reference: Domain 2 - IT Risk Assessment, Topic: Risk Quantification and Impact Analysis.

NEW QUESTION: 329
An organization is adopting block chain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?
A. Limited organizational knowledge of the underlying technology
B. Lack of commercial software support
C. Varying costs related to implementation and maintenance
D. Slow adoption of the technology across the financial industry
Answer: (SHOW ANSWER)
The greatest concern for a risk practitioner when an organization is adopting blockchain for a new financial system is the limited organizational knowledge of the underlying technology. Blockchain is a distributed ledger technology that enables secure and transparent transactions among multiple parties without the need for intermediaries or central authorities. Blockchain technology has many potential benefits for the financial sector, such as reducing costs, increasing efficiency, enhancing security, and improving trust. However, blockchain technology also poses many challenges and risks for the organization, such as technical complexity, interoperability issues, regulatory uncertainty, and cultural resistance. The limited organizational knowledge of the underlying technology is the greatest concern, because it affects the ability and readiness of the organization to adopt, implement, use, and maintain the blockchain system effectively and securely. The limited organizational knowledge could also result in poor decision-making, inadequate governance, insufficient training, and increased vulnerability to errors, fraud, or attacks. The other options are not as concerning as the limited organizational knowledge, although they may also pose some difficulties or limitations for the blockchain adoption. Lack of commercial software support, varying costs related to implementation and maintenance, and slow adoption of the technology across the financial industry are all factors that could affect the feasibility and sustainability of the blockchain system, but they do not directly affect the capability and maturity of the organization. References = 5

NEW QUESTION: 330

A vendor's planned maintenance schedule will cause a critical application to temporarily lose failover capabilities. Of the following, who should approve this proposed schedule?

freecram.net

A. IT infrastructure manager
B. Chief Risk Officer (CRO)
C. Business continuity manager
D. Business application owner
Answer: (SHOW ANSWER)
The business application owner is responsible for the operation and risk decisions related to the application. Since the loss of failover may impact business continuity, their approval is essential.
Reference:CRISC Manual - Domain 1, Slide 70, 214

NEW QUESTION: 331
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.
A. data logging and monitoring
B. data mining and analytics
C. data classification and labeling
D. data retention and destruction
Answer: (SHOW ANSWER)
The best way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for data retention and destruction. Data retention and destruction policies and procedures define the criteria, methods, and schedules for retaining and disposing of electronic data. They help to ensure that the electronic data is stored, managed, and deleted in a consistent, secure, and compliant manner. They also help to reduce the volume, complexity, and cost of retrieving electronic evidence, as they limit the scope, duration, and frequency of the data preservation and discovery process. The other options are not as effective as data retention and destruction policies and procedures, as they are related to the collection, analysis, or classification of electronic data, not the retention or destruction of electronic data. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 332

An application development team has a backlog of user requirements for a new system that will process insurance claim payments for customers. Which of the following should be the MOST important consideration for a risk-based review of the user requirements?

A. Number of claims affected by the user requirements

B. Number of customers impacted

C. Impact to the accuracy of claim calculation

D. Level of resources required to implement the user requirements

Answer: C (LEAVE A REPLY)

According to the CRISC Review Manual, one of the key objectives of risk identification is to assess the potential impact of risk events on the achievement of business objectives2. In this case, the business objective of the system is to process insurance claim payments for customers, which depends on the accuracy of claim calculation. Therefore, the impact to the accuracy of claim calculation should be the most important consideration for a risk-based review of the user requirements. The other options are less relevant or less critical for the business objective.

NEW QUESTION: 333

Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

A. Identify information security controls in the requirements analysis

B. Identify key risk indicators (KRIs) as process output.

C. Design key performance indicators (KPIs) for security in system specifications.

D. Include information security control specifications in business cases.

Answer: (SHOW ANSWER)

Information security risk factors are the sources of uncertainty that may affect the confidentiality, integrity, or availability of information assets within an organization. Information security risk factors can include threats, vulnerabilities, or impacts that may compromise the security of information assets. Information security risk factors should be mitigated when developing in-house applications, which are software applications that are designed, developed, and maintained by the organization itself, rather than by external vendors or providers. Mitigating information security risk factors when developing in-house applications canhelp prevent or reduce the occurrence or consequences of security incidents, such as data breaches, cyberattacks, unauthorized access, or data loss. The best way to ensure that information security risk factors are mitigated when developing in-house applications is to identify information security controls in the requirements analysis. The requirements analysis is the stage of the system development life cycle (SDLC) where the business needs and expectations of the application are defined and documented. The requirements analysis should include the functional and non-functional requirements of the application, such as the features, functions, performance, quality, reliability, and security of the application. Identifying information security controls in the requirements analysis can help ensure that the security requirements of the application are clearly specified and agreed upon by the stakeholders, and that they are aligned with the organization's security policies, standards, and regulations. Identifying information security controls in the requirements analysis can also help ensure that the security requirements are integrated into the design, development, testing, and deployment of the application, and that they are verified and validated throughout the SDLC. Identifying

information security controls in the requirements analysis can also help ensure that the security requirements are traceable, measurable, and manageable, and that they can be monitored and reviewed for effectiveness and efficiency. References = THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC), p. 2-3, System Development Life Cycle - GeeksforGeeks, 7.3: Systems Development Life Cycle - Engineering LibreTexts, What Is SDLC? 7 Phases of System Development Life Cycle - Intetics.

NEW QUESTION: 334
Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?
A. Updating the threat inventory with new threats
B. Automating log data analysis
C. Preventing the generation of false alerts
D. Determining threshold levels
Answer: (SHOW ANSWER)
* Key risk indicators (KRIs) are metrics that provide information about the level of exposure to a specific risk or a group of risks.
* The most important factor to the effective monitoring of KRIs is determining threshold levels. This means that the acceptable or unacceptable values or ranges of the KRIs are defined and agreed upon by the relevant stakeholders.
* Determining threshold levels helps to evaluate the actual performance and impact of the risks, compare them with the risk appetite and tolerance of the organization, identify any deviations or breaches that may require attention or action, and report them to the appropriate parties for decision making or improvement actions.
* The other options are not the most important factors to the effective monitoring of KRIs. They are either secondary or not essential for KRIs.
The references for this answer are:
* Risk IT Framework, page 15
* Information Technology & Security, page 9
* Risk Scenarios Starter Pack, page 7

NEW QUESTION: 335
Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?
A. Mean time to recover (MTTR)
B. IT system criticality classification
C. Incident management service level agreement (SLA)
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)
The best indicator of the risk appetite and tolerance level for the risk associated with business interruption caused by IT system failures is the recovery time objective (RTO). The RTO is the maximum acceptable time or duration that a business process or an IT system can be disrupted or interrupted before it causes unacceptable impact or harm to the business. The RTO reflects the risk appetite and tolerance level for the

business interruption risk, as it indicates how much disruption or interruption the business can tolerate or accept, and how quickly the business needs to resume or recover the business process or the IT system. The RTO also helps to determine the priorities and requirements for the business continuity and recovery planning, and to select and implement the appropriate continuity and recovery strategies and solutions. Mean time to recover (MTTR), IT system criticality classification, and incident management service level agreement (SLA) are not the best indicators of the risk appetite and tolerance level for the business interruption risk, as they are either the measures or the outcomes of the business continuity and recovery performance, and they do not directly indicate how much disruption or interruption the business can tolerate or accept. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 50

NEW QUESTION: 336
Which of the following is the MOST effective way to help ensure future risk levels do not exceed the organization's risk appetite?
A. Establishing a series of key risk indicators (KRIs).
B. Adding risk triggers to entries in the risk register.
C. Implementing key performance indicators (KPIs).
D. Developing contingency plans for key processes.
Answer: (SHOW ANSWER)
KRIs provide predictive metrics to monitor changes in risk levels, enabling timely interventions to maintain risks within the organization's appetite. This aligns with theRisk Monitoring and Reportingframework, which emphasizes proactive identification of risk thresholds.

NEW QUESTION: 337
A violation of segregation of duties is when the same:
A. user requests and tests the change prior to production.
B. user authorizes and monitors the change post-implementation.
C. programmer requests and tests the change prior to production.
D. programmer writes and promotes code into production.
Answer: (SHOW ANSWER)
A violation of segregation of duties is when the same person performs two or more conflicting tasks that could compromise the security or integrity of a system or process. In the context of IT risk management, segregation of duties aims to prevent fraud, errors, sabotage, theft, misuse of information, and other security breaches. One of the common categories of functions to be separated is the authorization function, which involves evaluating and approving transactions or changes. Another category is the custody function, which involves managing or accessing physical or digital assets. A programmer who writes and promotes code into production is performing both the authorization and the custody functions, which creates a high-risk conflict. The programmer could introduce malicious or erroneous code into the system without proper review or approval, and potentially cause harm to the organization or its stakeholders. Therefore, this scenario is a violation of segregation of duties. References = Segregation of Duties: Examples of Roles, Duties & Violations Separation of duties - Wikipedia Segregation of duties: prevent fraud and error - eftsure

NEW QUESTION: 338
Which of the following is the MOST important information to be communicated during security awareness training?
A. Management's expectations
B. Corporate risk profile
C. Recent security incidents
D. The current risk management capability
Answer: (SHOW ANSWER)
The most important information to be communicated during security awareness training is management's expectations. This will help to establish the security culture and behavior of the enterprise, and to align the staff's actions with the enterprise's objectives, policies, and standards. Management's expectations also provide the basis for measuring and evaluating the effectiveness of the security awareness program. Corporate risk profile, recent security incidents, and the current risk management capability are also important information to be communicated during security awareness training, but they are not as important as management's expectations. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.1.1.2, page 2291
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 642.

NEW QUESTION: 339
Which of We following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?
A. Establish baseline security configurations with the cloud service provider.
B. Require the cloud prowler 10 disclose past data privacy breaches.
C. Ensure the cloud service provider performs an annual risk assessment.
D. Specify cloud service provider liability for data privacy breaches in the contract
Answer: (SHOW ANSWER)
Specifying cloud service provider liability for data privacy breaches in the contract is the most effective control to address the risk associated with compromising data privacy within the cloud, because it establishes the roles and responsibilities of the cloud service provider and the customer in case of a data breach, and defines the compensation or remediation measures that the cloud service provider should provide. This control also creates an incentive for the cloud service provider to implement adequate security measures to protect the customer's data and comply with the relevant laws and regulations. The other options are not the most effective controls, although they may also be helpful in reducing the risk of data privacy breaches.
Establishing baseline security configurations with the cloud service provider, requiring the cloud service provider to disclose past data privacy breaches, and ensuring the cloud service provider performs an annual risk assessment are examples of preventive or detective controls that aim to reduce the likelihood or impact of a data breach, but they do not address the accountability or liability of the cloud service provider in case of a data breach. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 340

A user has contacted the risk practitioner regarding malware spreading laterally across the organization's corporate network. Which of the following is the risk practitioner's BEST course of action?

Freecram.net

A. Review all log files generated during the period of malicious activity.

B. Perform a root cause analysis.

C. Notify the cybersecurity incident response team.

D. Update the risk register.

Answer: (SHOW ANSWER)

Notifying the incident response team ensures immediate action to contain and remediate the malware spread, limiting further impact. This aligns withIncident Response and Containmentprotocols under risk management.

NEW QUESTION: 341

Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

A. To build an organizational risk-aware culture

B. To continuously improve risk management processes

C. To comply with legal and regulatory requirements

D. To identify gaps in risk management practices

Answer: B (LEAVE A REPLY)

* Global standards related to risk management are documents that provide the principles, guidelines, and best practices for managing risk in a consistent, effective, and efficient manner across different organizations, sectors, and regions12.
* The primary reason for a risk practitioner to use global standards related to risk management is to continuously improve risk management processes, which are the activities and tasks that enable the organization to identify, analyze, evaluate, treat, monitor, and communicate the risks that may affect its objectives, performance, and value creation34.
* Continuously improving risk management processes is the primary reason because it helps the organization to enhance its risk management capabilities and maturity, and to adapt to the changing risk environment and stakeholder expectations34.
* Continuously improving risk management processes is also the primary reason because it supports the achievement of the organization's goals and the delivery of value to the stakeholders, which are the ultimate purpose and outcome of risk management34.
* The other options are not the primary reason, but rather possible benefits or objectives that may result from using global standards related to risk management. For example:
* Building an organizational risk-aware culture is a benefit of using global standards related to risk management that involves creating and maintaining a shared understanding, attitude, and behavior towards risk among the organization's employees and leaders, and fostering a culture of accountability, transparency, and learning34. However, this benefit is not the primary reason because it is an enabler and a consequence of continuously improving risk management processes, rather than a driver or a goal34.

* Complying with legal and regulatory requirements is an objective of using global standards related to risk management that involves meeting and exceeding the expectations and obligations of the external authorities or bodies that govern or oversee the organization's activities and operations, such as laws, regulations, standards, or contracts34. However, this objective is not the primary reason because it is a constraint and a challenge of continuously improving risk management processes, rather than a motivation or a benefit34.
* Identifying gaps in risk management practices is an objective of using global standards related to risk management that involves assessing and comparing the current and desired state of the organization's risk management processes, and identifying the areas or aspects that need to be improved or addressed34. However, this objective is not the primary reason because it is a step and a tool of continuously improving risk management processes, rather than a reason or a result34. References =
* 1: ISO - ISO 31000 - Risk management1
* 2: Risk Management Standards2
* 3: Risk IT Framework, ISACA, 2009
* 4: IT Risk Management Framework, University of Toronto, 2017

NEW QUESTION: 342
When creating a program to manage data privacy risk, which of the following is MOST important to ensure that the program is successful?
A. Compliance with industry frameworks
B. Alignment with applicable legal and regulatory requirements
C. Approval of mitigating and compensating controls
D. Adoption of mission and vision statements
Answer: (SHOW ANSWER)
Privacy risk management programs must align withspecific regulatory obligations(e.g., GDPR, HIPAA) to be effective and compliant. Legal alignment defines scope, control requirements, and accountability.
Reference:CRISC Manual - Domain 1, Slide 106-108

NEW QUESTION: 343
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?
A. Reviewing the results of independent audits
B. Performing a site visit to the cloud provider's data center
C. Performing a due diligence review
D. Conducting a risk workshop with key stakeholders
Answer: (SHOW ANSWER)
The most helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment is conducting a risk workshop with key stakeholders. A risk workshop is a facilitated session that involves brainstorming, discussing, and analyzing the potential risks and opportunities related to a specific topic or project. A risk workshop helps to identify and prioritize the most relevant and significant risk scenarios, as well as to explore the possible causes, impacts, and responses. A risk workshop also

helps to engage and align the key stakeholders, such as the business owners, IT managers, cloud providers, and risk experts, and to leverage their knowledge, experience, and perspectives. The other options are not as helpful as conducting a risk workshop, although they may provide some input or information for the risk scenario development. Reviewing the results of independent audits, performing a site visit to the cloud provider's data center, and performing a due diligence review are all activities that can help to assess the current state and performance of the cloud environment, but they do not necessarily generate or evaluate the risk scenarios. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page
4-13.

NEW QUESTION: 344
An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?
A. Employ security guards.
B. Conduct security awareness training.
C. Install security cameras.
D. Require security access badges.
Answer: B (LEAVE A REPLY)
Social engineering is a technique that involves manipulating or deceiving people into performing actions or divulging information that may compromise the security of an organization or its data12.
Entry into an organization's secured physical premises is a form of physical access that allows an unauthorized individual to access, steal, or damage the organization's assets, such as equipment, documents, or systems34.
The best way to prevent future occurrences of social engineering entry into an organization's secured physical premises is to conduct security awareness training, which is an educational program that aims to equip the organization's employees with the knowledge and skills they need to protect the organization's data and sensitive information from cyber threats, such as hacking, phishing, or other breaches56.
Security awareness training is the best way because it helps the employees to recognize and resist the common and emerging social engineering techniques, such as tailgating, impersonation, or pretexting, that may be used by the attackers to gain physical access to the organization's premises56.
Security awareness training is also the best way because it fosters a culture of security and responsibility among the employees, and encourages them to follow the best practices and policies for physical security, such as locking the doors, verifying the identity of visitors, or reporting any suspicious activities or incidents56.
The other options are not the best way, but rather possible measures or controls that may supplement or enhance the security awareness training. For example:
Employing security guards is a measure that involves hiring or contracting professional personnel who are trained and authorized to monitor, patrol, and protect the organization's premises from unauthorized access or intrusion78. However, this measure is not the best way because it may not be sufficient or effective to prevent or deter all types of social engineering attacks, especially if the attackers are able to bypass, deceive, or coerce the security guards78.

Installing security cameras is a control that involves using electronic devices that capture and record the visual images of the organization's premises, and provide evidence or alerts of any unauthorized access or activity .
However, this control is not the best way because it is reactive rather than proactive, and may not prevent or stop the social engineering attacks before they cause any harm or damage to the organization .
Requiring security access badges is a control that involves using physical or electronic cards that identify and authenticate the employees or authorized visitors who are allowed to enter the organization's premises, and restrict or deny the access to anyone else . However, this control is not the best way because it may not be foolproof or reliable to prevent or detect the social engineering attacks, especially if the attackers are able to steal, forge, or clone the security access badges . References =
1: What is Social Engineering? | Types & Examples of Social Engineering Attacks1
2: Social Engineering: What It Is and How to Prevent It | Digital Guardian2
3: What is physical Social Engineering and why is it important? - Integrity3603
4: What Is Tailgating (Piggybacking) In Cyber Security? - Wlan Labs4
5: What Is Security Awareness Training and Why Is It Important? - Kaspersky5
6: Security Awareness Training - Cybersecurity Education Online | Proofpoint US6
7: Security Guard - Wikipedia7
8: Security Guard Services - Allied Universal8
Security Camera - Wikipedia
Security Camera Systems - The Home Depot
Access Badge - Wikipedia
Access Control Systems - HID Global

NEW QUESTION: 345
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?
A. Key risk indicators (KRIs) are developed for key IT risk scenarios
B. IT risk scenarios are assessed by the enterprise risk management team
C. Risk appetites for IT risk scenarios are approved by key business stakeholders.
D. IT risk scenarios are developed in the context of organizational objectives.
Answer: (SHOW ANSWER)
IT risk scenarios are hypothetical situations that describe how IT-related events or incidents could adversely affect an organization's objectives, assets, or operations. IT risk scenarios can help to identify, analyze, and prioritize IT risks, and to develop appropriate responses and controls1.
An enterprise-wide risk register is a document that records and tracks the significant risks that an organization faces across its various functions, processes, and activities. An enterprise-wide risk register can help to provide a comprehensive and consistent view of the organization's risk profile, and to support the decision making and reporting of the risk management function2.
The best practice that facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register is to develop IT risk scenarios in the context of organizational objectives. This means that IT risk scenarios should be aligned with and derived from the organization's strategic goals, mission, vision, and values. IT risk

scenarios should also consider the interdependencies and interactions between IT and other business domains, and the potential impact of IT risks on the organization's performance and reputation3.
By developing IT risk scenarios in the context of organizational objectives, the organization can ensure that the IT risk scenarios are relevant, realistic, and meaningful for the enterprise-wide risk management. The organization can also ensure that the IT risk scenarios are consistent and comparable with other types of risk scenarios, such as financial, operational, or reputational risk scenarios. This can facilitate the integration and consolidation of IT risk scenarios into the enterprise-wide risk register, and enable a holistic and balanced assessment and reporting of the organization's risks4.
The other options are not as effective as developing IT risk scenarios in the context of organizational objectives for incorporating IT risk scenarios into the enterprise-wide risk register. Developing key risk indicators (KRIs) for key IT risk scenarios can help to monitor and measure the IT risk exposure and performance, but it does not ensure that the IT risk scenarios are aligned with the organizational objectives or integrated with other risk scenarios. Assessing IT risk scenarios by the enterprise risk management team can help to validate and prioritize the IT risk scenarios, but it does not ensure that the IT risk scenarios are derived from the organizational objectives or consistent with other risk scenarios. Approving risk appetites for IT risk scenarios by key business stakeholders can help to establish the acceptable level of IT risk taking and tolerance, but it does not ensure that the IT risk scenarios are based on the organizational objectives or comparable with other risk scenarios. References = IT Risk Scenario Development - ISACA Risk Register - ISACA Identifying Risks and Scenarios Threatening the Organization as an Enterprise - A New Enterprise Risk Identification Framework Risk Register 2021-2022 - UNECE
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 346
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?
A. Align business objectives with risk appetite.
B. Enable risk-based decision making.
C. Design and implement risk response action plans.
D. Update risk responses in the risk register
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, the primary purpose of periodically reviewing an organization's risk profile is to enable risk-based decision making, because it helps to ensure that the risk information is current, relevant, and accurate. The risk profile is a snapshot of the organization's risk exposure at a given point in time, based on the risk identification, analysis, and evaluation processes. Periodically reviewing the risk profile allows the organization to monitor the changes in the risk environment, the effectiveness of the risk responses, and the impact of the risk events. This enables the organization to make informed decisions about the risk management strategies and priorities. The other options are not the primary purpose of periodically reviewing the risk profile, as they are related to other aspects of the risk management process. Aligning business objectives with risk appetite is the purpose of establishing the risk context, which defines the scope and boundaries of the risk management activities. Designing and implementing risk response action plans is the purpose of the risk response process, which involves selecting and executing the appropriate risk responses. Updating risk responses in the risk register is the outcome of the risk monitoring

and reporting process, which involves tracking the risk performance and communicating the risk information to the stakeholders. References = CRISC Review Manual, 7th Edition, Chapter 2, Section 2.2.4, page 86.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 347
Determining if organizational risk is tolerable requires:
A. mapping residual risk with cost of controls
B. comparing against regulatory requirements
C. comparing industry risk appetite with the organizations.
D. understanding the organization's risk appetite.
Answer: (SHOW ANSWER)
Determining if organizational risk is tolerable requires understanding the organization's risk appetite, which is the amount and type of risk that the organization is willing to accept or pursue in order to achieve its objectives1. Understanding the organization's risk appetite can help to:
* Define and communicate the risk tolerance, which is the acceptable or unacceptable level of risk for each risk category or scenario2.
* Guide and align the risk identification, analysis, evaluation, and treatment processes, and ensure that the risks are consistent and proportional to the risk appetite3.
* Measure and monitor the risk performance and outcome, and ensure that the residual risk (the risk that remains after the risk responses) is within the risk appetite, or take corrective actions if needed4.
The other options are not the best ways to determine if organizational risk is tolerable, because:
* Mapping residual risk with cost of controls is a useful but not sufficient way to determine if organizational risk is tolerable, as it provides a quantitative analysis of the trade-off between the risk level and the risk response cost5. However, mapping residual risk with cost of controls does not consider the qualitative aspects of the risk, such as the impact on the organization's strategy, culture, or reputation.
* Comparing against regulatory requirements is a necessary but not sufficient way to determine if organizational risk is tolerable, as it ensures that the organization complies with the applicable laws, rules, or standards that govern its activities and operations6. However, comparing against regulatory requirements does not guarantee that the organization meets its own objectives and expectations, which may be higher or lower than the regulatory requirements.
* Comparing industry risk appetite with the organization's risk appetite is a helpful but not sufficient way to determine if organizational risk is tolerable, as it provides a reference or a standard for benchmarking the organization's risk level and performance with its peers or competitors7. However, comparing industry risk

appetite with the organization's risk appetite does not ensure that the organization addresses its specific or unique risks, which may differ from the industry risks.
References =
* Risk Appetite - CIO Wiki
* Risk Tolerance - CIO Wiki
* Risk Management Process - CIO Wiki
* Risk Monitoring - CIO Wiki
* Residual Risk - CIO Wiki
* Regulatory Compliance - CIO Wiki
* Benchmarking - CIO Wiki
* Risk and Information Systems Control documents and learning resources by ISACA

NEW QUESTION: 348
An organization uses a web application hosted by a cloud service that is populated by data sent to the vendor via email on a monthly basis. Which of the following should be the FIRST consideration when analyzing the risk associated with the application?
A. Whether the service provider's data center is located in the same country
B. Whether the data sent by email has been encrypted
C. Whether the data has been appropriately classified
D. Whether the service provider contract allows right of onsite audit
Answer: (SHOW ANSWER)
Data classification is the process of assigning labels or categories to data based on its sensitivity, value, and criticality to the organization. Data classification is the first consideration when analyzing the risk associated with the web application hosted by a cloud service, as it determines the level of protection and controls required for the data. Data classification can help the organization to comply with legal, regulatory, and contractual obligations, such as GDPR, CCPA, and PCI DSS, and to prevent data breaches, leaks, or losses. Data classification can also help the organization to evaluate the suitability and trustworthiness of the cloud service provider, and to negotiate the terms and conditions of the service level agreement (SLA).
References:
*ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, p. 141
*ISACA, Data Classification: What It Is, Why You Should Care and How to Perform It2

NEW QUESTION: 349
Which of the following is the MOST important reason to revisit a previously accepted risk?
A. To update risk ownership
B. To review the risk acceptance with new stakeholders
C. To ensure risk levels have not changed
D. To ensure controls are still operating effectively
Answer: (SHOW ANSWER)

The most important reason to revisit a previously accepted risk is to ensure that the risk levels have not changed. A previously accepted risk is a risk that the organization has decided to tolerate or retain without taking any further action, because the risk is either low or unavoidable, or the cost or effort of mitigation outweighs the potential benefit. However, risk acceptance is not a static or permanent decision, as the risk levels may change over time due to various factors, such as new threats, vulnerabilities, impacts, or opportunities. Therefore, it is essential to revisit a previously accepted risk periodically or when there is a significant change in the internal or external environment, to verify that the risk is still within the acceptable range and that the risk acceptance rationale is still valid. If the risk levels have increased or decreased, the organization may need to revise the risk acceptance decision and consider other risk response options, such as avoidance, reduction, sharing, or exploitation. The other options are not the most important reason to revisit a previously accepted risk, although they may be relevant or necessary depending on the context and nature of the risk. Updating risk ownership is a part of the risk governance process, which ensures that the roles and responsibilities for managing the risk are clearly defined and assigned, but it does not affect the risk levels or the risk acceptance decision. Reviewing the risk acceptance with new stakeholders is a part of the risk communication process, which ensures that the risk information and the risk acceptance rationale are shared and understood by the relevant parties, but it does not change the risk levels or the risk acceptance decision.
Ensuring that the controls are still operating effectively is a part of the risk monitoring and review process, which ensures that the risk response actions are implemented and maintained properly, but it does not apply to the accepted risks, as they do not have any additional controls. References = Understanding Accepted Risk - SC Dashboard | Tenable, Risk Acceptance - ENISA, Accepting Risk - Overview, Advantages, Disadvantages, Alternatives

NEW QUESTION: 350

Which of the following BEST enables an organization to determine whether risk management is aligned with its goals and objectives?

Freecram.net

A. The organization has approved policies that provide operational boundaries.
B. Organizational controls are in place to effectively manage risk appetite.
C. Environmental changes that impact risk are continually evaluated.
D. The organization has an approved enterprise architecture (EA) program.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, enterprise architecture (EA) is a comprehensive framework that defines the structure and operation of an organization, including its business processes, information systems, technology infrastructure, organizational structure, and strategic objectives2. An EA program is a set of principles, policies, standards, and guidelines that govern the development and implementation of the EA3. By having an approved EA program, an organization can ensure that its risk management is aligned with its goals and objectives, as the EA provides a clear and consistent vision of the desired state and direction of the organization, as well as the means to achieve and measure it4. The EA also helps to identify and prioritize the risks and opportunities that may affect the organization's performance and resilience. The other options are not as effective or relevant as option D, as they do not directly relate to the alignment of risk management with organizational goals and objectives. Option A, having approved policies that provide

operational boundaries, is more related to the governance and compliance of risk management, not its alignment. Option B, having organizational controls to manage risk appetite, is more related to the implementation and monitoring of risk management, not its alignment. Option C, continually evaluating environmental changes that impact risk, is more related to the identification and assessment of risk management, not its alignment.

NEW QUESTION: 351
The MOST appropriate key performance indicator (KPI) to communicate the effectiveness of an enterprise IT risk management program is:
A. The percentage of risk scenarios that are within organizational tolerance
B. The percentage of IT staff trained in risk management
C. The number of critical business services covered by a risk assessment
D. The amount of IT risk realized that impacted the business
Answer: (SHOW ANSWER)
The KPI that best measures effectiveness of risk management is one that shows risk alignment with tolerance levels.
CRISC defines:
"Risk management effectiveness is demonstrated when risk scenarios are managed within the organization's defined tolerance."
* B and C are activity-based, not outcome-based.
* D measures realized losses, not ongoing control success.
Hence, A. The percentage of risk scenarios within organizational tolerance directly reflects program effectiveness.
CRISC Reference: Domain 4 - Risk and Control Monitoring and Reporting, Topic: Key Risk and Performance Indicators.

NEW QUESTION: 352
Which of the following BEST indicates that risk management is embedded into the responsibilities of all employees?
A. The number of incidents has decreased over time
B. Industry benchmarking is performed on an annual basis
C. Risk management practices are audited on an annual basis
D. Risk management practices are incorporated into business processes
Answer: (SHOW ANSWER)
Embedding risk management into day-to-day business processes reflects organizational maturity and integration. It ensures employees consider risk in operational decisions and continuously support the risk management framework.
Reference:CRISC Manual - Domain 1, Slide 84-87

NEW QUESTION: 353
Which of the following would require updates to an organization's IT risk register?

A. Discovery of an ineffectively designed key IT control
B. Management review of key risk indicators (KRIs)
C. Changes to the team responsible for maintaining the register
D. Completion of the latest internal audit
Answer: (SHOW ANSWER)
An IT risk register is a document that records and tracks the identified IT risks, their likelihood, impact, and mitigation strategies. It is a living document that needs to be updated regularly to reflect the current risk profile of the organization. One of the situations that would require updates to the IT risk register is the discovery of an ineffectively designed key IT control, as this would increase the likelihood or impact of the related IT risk. Management review of key risk indicators (KRIs), changes to the team responsible for maintaining the register, and completion of the latest internal audit are not reasons to update the IT risk register, as they do not affect the identified IT risks or their mitigation strategies. References = [CRISC Review Manual (Digital Version)], page 97; CRISC: Certified in Risk & Information Systems Control Sample Questions, question 198.

NEW QUESTION: 354
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?
A. Prioritize risk response options
B. Reduce likelihood.
C. Address more than one risk response
D. Reduce impact
Answer: (SHOW ANSWER)
The most important objective from a cost perspective for considering aggregated risk responses in an organization is to address more than one risk response. Aggregated risk responses are risk responses that can affect multiple risks or objectives simultaneously. By addressing more than one risk response, the organization can achieve cost efficiency and effectiveness in risk management. Prioritizing risk response options, reducing likelihood, and reducing impact are other possible objectives, but they are not as important from a cost perspective as addressing more than one risk response. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 10; CRISC Review Manual, 6th Edition, page 140.

NEW QUESTION: 355
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?
A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
B. Implement a key performance indicator (KPI) to monitor the existing control performance.
C. Accept the residual risk in its entirety and obtain executive management approval.
D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.
Answer: (SHOW ANSWER)

Implementing controls to bring the risk to a level within appetite and accept the residual risk is the best recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated, as it helps to balance the costs and benefits of the risk management and control processes, and to align them with the organizational strategy and objectives. A risk and control assessment is a process of identifying, analyzing, and evaluating the risks and controls associated with a specific activity, process, or objective. A risk scenario is a description of a possible event or situation that could cause harm or loss to the organization or its stakeholders. A risk scenario can only be partially mitigated when the existing or proposed controls are not sufficient or effective to reduce the risk to an acceptable level.
A risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. A residual risk is the risk that remains after the implementation of controls or risk treatments. Implementing controls to bring the risk to a level within appetite and accept the residual risk helps to provide the following benefits:
It enables a data-driven and evidence-based approach to risk management and reporting, rather than relying on subjective or qualitative judgments.
It facilitates a consistent and standardized way of measuring and communicating risk levels and exposure across the organization and to the external stakeholders.
It supports the development and implementation of effective and efficient risk response and mitigation strategies and actions that are aligned with the business risk appetite and objectives.
It provides feedback and learning opportunities for the risk management and control processes, and helps to foster a culture of continuous improvement and innovation.
The other options are not the best recommendations to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated. Implementing a key performance indicator (KPI) to monitor the existing control performance is a useful method to measure and monitor the effectiveness and efficiency of the controls, but it does not address the residual risk or the risk appetite. Accepting the residual risk in its entirety and obtaining executive management approval is a possible option to deal with the risk scenario, but it may expose the organization to excessive or unacceptable risk, and it may not comply with the legal or regulatory obligations or requirements. Separating the risk into multiple components and avoiding the risk components that cannot be mitigated is a possible option to deal with the risk scenario, but it may not be feasible or practical, and it may create new or additional risks or challenges.
References = Risk and Control Self-Assessment (RCSA) - Management Study Guide, IT Risk Resources | ISACA, Risk Mitigation: What It Is and How to Implement It (Free Templates ...

NEW QUESTION: 356
An organization's decision to remain noncompliant with certain laws or regulations is MOST likely influenced by:
A. The region in which the organization operates.
B. Established business culture.
C. Risk appetite set by senior management.
D. Identified business process controls.
Answer: (SHOW ANSWER)

Risk appetite determined by senior management reflects the enterprise's willingness to accept certain levels of risk, including noncompliance. This decision underscores the strategic trade-offs made in risk management, a key element inGovernance and Risk Policy Alignment.

NEW QUESTION: 357
Which of the following is a business asset for an organization that runs only in a Software as a Service (SaaS) cloud computing environment?
A. Hosted data
B. Platforms
C. Containers
D. Security logs
Answer: (SHOW ANSWER)
In a SaaS environment, the provider manages infrastructure and platforms. The primary asset that remains under the organization's control is its hosted data. Hence, data is the key business asset.
Reference:CRISC Manual - Domain 1: Governance, Slide 41

NEW QUESTION: 358
Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?
A. The KRIs' source data lacks integrity.
B. The KRIs are not automated.
C. The KRIs are not quantitative.
D. The KRIs do not allow for trend analysis.
Answer: (SHOW ANSWER)
The greatest concern for a risk practitioner reviewing current key risk indicators (KRIs) is that the KRIs' source data lacks integrity, as this means that the data is inaccurate, incomplete, inconsistent, or outdated, and therefore cannot provide reliable and valid information on the risk level and performance. The KRIs are metrics that measure and monitor the changes in the risk exposure and the effectiveness of the risk response over time. The KRIs' source data should be collected and verified from credible and relevant sources, and should be updated and maintained regularly. The KRIs' source data should also be aligned and integrated with the enterprise's data governance and quality standards. The other options are not the greatest concerns for a risk practitioner reviewing current key risk indicators (KRIs), although they may pose some challenges or limitations. The KRIs are not automated is a concern for the efficiency and timeliness of the KRI reporting and analysis, but it does not affect the integrity of the KRI source data. The KRIs are not quantitative is a concern for the objectivity and comparability of the KRI measurement and prioritization, but it does not affect the integrity of the KRI source data. The KRIs do not allow for trend analysis is a concern for the usefulness and relevance of the KRI communication and decision making, but it does not affect the integrity of the KRI source data. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk and Control Monitoring and Reporting, page 183.

NEW QUESTION: 359

A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

A. identification.

B. treatment.

C. communication.

D. assessment

Answer: (SHOW ANSWER)

A risk heat map is a graphical tool that displays the results of a risk analysis in a matrix format, using colors and symbols to indicate the level and priority of the risks. A risk heat map can show the distribution and comparison of the risks based on various criteria, such as likelihood, impact, category, source, etc.

A risk heat map is most commonly used as part of an IT risk analysis to facilitate risk assessment, which is the process of determining the significance and urgency of the risks that may affect the organization's objectives and operations. Risk assessment involves measuring and comparing the likelihood and impact of various risk scenarios, and prioritizing them based on their magnitude and importance.

A risk heat map can help to facilitate risk assessment by providing a visual and intuitive representation of the risk profile, and highlighting the most critical and relevant risks that need to be addressed or monitored. A risk heat map can also help to communicate and report the riskanalysis results to different stakeholders, and to support the decision making and planning for the risk response and treatment.

The other options are not the most common uses of a risk heat map as part of an IT risk analysis, because they do not address the main purpose and benefit of a risk heat map, which is to facilitate risk assessment.

Risk identification is the process of finding and describing the risks that may affect the organization's objectives and operations. Risk identification involves defining the risk sources, events, causes, and impacts, and documenting them in a risk register. A risk heat map is not commonly used to facilitate risk identification, because it does not provide the detailed and comprehensive information that is needed to identify and describe the risks, and it may not cover all the relevant or potential risks that may exist or emerge.

Risk treatment is the process of selecting and implementing the appropriate actions or plans to address the risks that have been identified, analyzed, and evaluated. Risk treatment involves choosing one of the following types of risk responses: mitigate, transfer, avoid, or accept. A risk heat map is not commonly used to facilitate risk treatment, because it does not provide the specific and feasible information that is needed to select and implement the risk responses, and it may not reflect the cost-benefit or feasibility analysis of the risk responses.

Risk communication is the process of exchanging and sharing the information and knowledge about the risks and their responses among the relevant stakeholders. Risk communication involves informing, consulting, and involving the stakeholders in the risk management process, and ensuring that they understand and agree on the risk objectives, criteria, and outcomes. A risk heat map is not commonly used to facilitate risk communication, because it does not provide the complete and accurate information that is needed to communicate and share the risks and their responses, and it may not address the different needs, expectations, and perspectives of the stakeholders. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-59, 62-63

ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 169 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 360

After the implementation of a blockchain solution, a risk practitioner discovers noncompliance with new industry regulations. Which of the following is the MOST important course of action prior to informing senior management?

Freecram.net

A. Evaluate the design effectiveness of existing controls.

B. Implement compensating controls.

C. Evaluate the industry response to the new regulations.

D. Evaluate the potential impact.

Answer: (SHOW ANSWER)

Before escalating to senior management, a risk practitioner must understand how serious the issue is for the enterprise. That means first assessing the business impact of the noncompliance (financial, regulatory, reputational, operational) so that management is given contextualized information rather than just "we are noncompliant." In ISACA's CRISC framework, risk assessment always requires understanding likelihood and impact before risk response and escalation decisions. Evaluating the potential impact allows:

* Identification of which processes, customers, or jurisdictions are affected.
* Estimation of the magnitude of legal/regulatory exposure.
* Understanding whether immediate containment actions are needed.
* Preparation of meaningful options and recommendations for senior management.

Options A and B (evaluating controls and implementing compensating controls) are important later, as part of risk response / treatment. However, without first knowing the impact, you cannot determine how urgent or extensive the remedial actions must be.

Option C (evaluating industry response) may be useful for benchmarking, but it does not help the enterprise understand its own specific exposure and obligations and therefore is secondary to an internal impact assessment.

This aligns with CRISC guidance that the primary result of a risk assessment is input for risk-aware decisions and that risk professionals must assess likelihood and impact to determine risk significance before escalation and treatment (see the risk assessment and risk profile-related guidance in your CRISC notes).

NEW QUESTION: 361

Which of the following is the MOST important document regarding the treatment of sensitive data?

A. Encryption policy

B. Organization risk profile

C. Digital rights management policy

D. Information classification policy

Answer: (SHOW ANSWER)

The information classification policy is the most important document regarding the treatment of sensitive data, because it defines the categories and criteria for classifying data according to their sensitivity, confidentiality, and value to the organization, and specifies the appropriate handling and protection measures for each category. Sensitive data are data that contain personal, proprietary, or confidential information that may cause harm or damage to the organization or its stakeholders if disclosed, modified, or destroyed

without authorization. An information classification policy helps to ensure that sensitive data are identified and treated in a consistent and secure manner, and that the organization complies with the applicable laws and regulations regarding data protection and privacy. An encryption policy, an organization risk profile, and a digital rights management policy are all useful documents for the treatment of sensitive data, but they are not the most important document, as they do not directly address the classification and handling of sensitive data.
References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 362
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?
A. Data encryption has not been applied to all sensitive data across the organization.
B. There are many data assets across the organization that need to be classified.
C. Changes to information handling procedures are not documented.
D. Changes to data sensitivity during the data life cycle have not been considered.
Answer: (SHOW ANSWER)
Changes to data sensitivity during the data life cycle present the greatest risk for a global organization when implementing a data classification policy, as they may result in data being under-protected or over-protected, leading to potential data breaches, compliance violations, or inefficiencies. Data sensitivity refers to the level of confidentiality, integrity, and availability that the data requires, and it may changedepending on the data's creation, storage, processing,transmission, or disposal. A data classification policy should consider the changes to data sensitivity during the data life cycle and ensure that the appropriate controls and procedures are applied at each stage. Data encryption not applied to all sensitive data, many data assets that need to be classified, and changes to information handling procedures not documented are not the greatest risks, as they do not affect the data classification policy itself, but rather the implementation or execution of the policy.
References = CRISC Certified in Risk and Information Systems Control - Question211; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 211.

NEW QUESTION: 363
Within the three lines of defense model, the accountability for the system of internal control resides with:
A. the chief information officer (CIO).
B. the board of directors
C. enterprise risk management

D. the risk practitioner

Answer: (SHOW ANSWER)

* The three lines of defense model is a framework that describes the roles and responsibilities of different functions in an organization for managing risks and controls.
* The first line of defense is the operational management, which is responsible for implementing and maintaining effective controls, identifying and assessing risks, and reporting on risk and control performance.
* The second line of defense is the risk management and compliance functions, which are responsible for establishing and overseeing the risk management framework, providing guidance and support to the operational management, and monitoring and reporting on risk and compliance issues.
* The third line of defense is the internal audit function, which is responsible for providing independent and objective assurance on the adequacy and effectiveness of the risk management and control system, and recommending improvements.
* Within the three lines of defense model, the accountability for the system of internal control resides with the chief information officer (CIO). The CIO is the senior executive who oversees the IT function of the organization, and is responsible for ensuring that the IT risks and controls are aligned with the business objectives and strategies, and are integrated with the enterprise risk management and governance processes.

The references for this answer are:

* Risk IT Framework, page 20
* Information Technology & Security, page 14
* Risk Scenarios Starter Pack, page 12

NEW QUESTION: 364

Which of the following is the PRIMARY role of the first line of defense with respect to information security policies?

A. Audit the implementation of the information security policy.

B. Draft the information security policy.

C. Approve the information security policy.

D. Implement controls in response to the policy requirements.

Answer: (SHOW ANSWER)

NEW QUESTION: 365

Which of the following metrics is BEST used to communicate to senior management that the control environment manages risk within appetite and tolerance?

A. Number of security incidents

B. Reduction in control expenditures

C. Number of risk responses executed

D. Reduction in residual risk

Answer: (SHOW ANSWER)

Residual riskrepresents the amount of risk remaining after controls have been applied. Tracking its reduction over time directly indicates whether controls are effectively reducing risk to withintolerance limits.

Reference:CRISC Manual - Domain 4, Slide 384-386

NEW QUESTION: 366
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?
A. The report was provided directly from the vendor.
B. The risk associated with multiple control gaps was accepted.
C. The control owners disagreed with the auditor's recommendations.
D. The controls had recurring noncompliance.
Answer: (SHOW ANSWER)
The most concerning issue when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment is that the controls had recurring noncompliance. This indicates that the vendor's controls are not operating as intended or designed, and that the vendor is not taking corrective actions to address the control deficiencies. This can increase the risk exposure and liability for the organization that outsources the service or function to the vendor. The report being provided directly from the vendor, the risk associated with multiple control gaps being accepted, and the control owners disagreeing with the auditor's recommendations are other possible issues, but they are not as critical as the recurring noncompliance. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 11; CRISC Review Manual, 6th Edition, page 144.

NEW QUESTION: 367
Which of the following BEST facilitates the development of effective IT risk scenarios?
A. Utilization of a cross-functional team
B. Participation by IT subject matter experts
C. Integration of contingency planning
D. Validation by senior management
Answer: (SHOW ANSWER)
The best way to facilitate the development of effective IT risk scenarios is to utilize a cross-functional team. A cross-functional team is a group of people with different skills, expertise, and perspectives who work together to achieve a common goal. A cross-functional team can help to create realistic, comprehensive, and relevant IT risk scenarios by bringing diverse knowledge, experience, and insights from various domains and functions. A cross-functional team can also help to identify and address the interdependencies, interactions, and impacts of IT risks across the organization. The other options are not the best ways to facilitate the development of effective IT risk scenarios, although they may be useful or necessary depending on the context and nature of the IT risks. Participation by IT subject matter experts is important, but it is not sufficient, as IT risks may affect or be affected by non-IT factors and stakeholders. Integration of contingency planning is a part of the risk response process, which follows the risk scenario development process, but it is not the same as creating the risk scenarios. Validation by senior management is a quality assurance step that ensures the accuracy and completeness of the risk scenarios, but it is not the same as facilitating the development of the risk scenarios. References = Six Steps to Using Risk Scenarios for Improved Risk Management, IT Risk Scenarios - Morland-Austin, IT Risk Resources | ISACA

NEW QUESTION: 368
What should a risk practitioner do FIRST when a shadow IT application is identified in a business owner's business impact analysis (BIA)?
A. Include the application in the business continuity plan (BCP).
B. Determine the business purpose of the application.
C. Segregate the application from the network.
D. Report the finding to management.
Answer: (SHOW ANSWER)
Determining the business purpose of the application is the first thing that a risk practitioner should do when a shadow IT application is identified in a business owner's business impact analysis (BIA), because it helps to understand the rationale and value of the application, and the potential risks and issues that it may introduce or affect. A shadow IT application is an IT system or application that is used by the business units or employees without the knowledge or approval of the IT department or management. A shadow IT application may offer benefits such as convenience, efficiency, or innovation, but it may also pose risks such as security breaches, data loss, compatibility issues, or regulatory non-compliance. A BIA is a process of analyzing the potential impact of disruption to the critical business functions or processes, and identifying the recovery priorities and requirements. A BIA may reveal the existence of a shadow IT application, as it may be used to support or enable a critical business function or process. Determining the business purpose of the application is the first thing to do, as it helps to evaluate the necessity and suitability of the application, and to plan the appropriate actions to address the shadow IT application. Including the application in the business continuity plan (BCP), segregating the application from the network, and reporting the finding to management are all possible things to do after determining the business purpose of the application, but they are not the first thing to do, as they depend on the results of the evaluation of the application. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 143

NEW QUESTION: 369
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?
A. Review vendor control self-assessments (CSA).
B. Review vendor service level agreement (SLA) metrics.
C. Require independent control assessments.
D. Obtain vendor references from existing customers.
Answer: (SHOW ANSWER)
The best way to provide assurance of the effectiveness of vendor security controls is to require independent control assessments. Independent control assessments are evaluations of the vendor's security controls by a third-party auditor or assessor, such as an external auditor, a certification body, or a testing laboratory. Independent control assessments provide an objective and unbiased opinion on the adequacy and performance of the vendor's security controls, as well as the compliance with relevant standards and regulations.
Independent control assessments can also provide evidence and assurance to the customers of the vendor's security posture and capabilities. Reviewing vendor control self-assessments (CSA), vendor service level

agreement (SLA) metrics, or vendor references from existing customers are not as reliable or credible as independent control assessments, because they may be biased, incomplete, or outdated.

NEW QUESTION: 370

Which of the following is the PRIMARY advantage of having a single integrated business continuity plan (BCP) rather than each business unit developing its own BCP?

Pass4Train.net

A. It enables effective BCP maintenance and updates to reflect organizational changes.

B. It provides assurance of timely business process response and effectiveness.

C. It decreases the risk of downtime and operational losses in the event of a disruption.

D. It supports effective use of resources and provides reasonable confidence of recoverability.

Answer: (SHOW ANSWER)

NEW QUESTION: 371

When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?

A. Perform a background check on the vendor.

B. Require the vendor to sign a nondisclosure agreement.

C. Require the vendor to have liability insurance.

D. Clearly define the project scope

Answer: (SHOW ANSWER)

When using a third party to perform penetration testing, the most important control to minimize operational impact is to clearly define the project scope. This means specifying the objectives, boundaries, methods, and deliverables of the testing, as well as the roles and responsibilities of the parties involved. A clear project scope helps to avoid misunderstandings, conflicts, and disruptions that could compromise the security, availability, or integrity of the systems under test. It also helps to ensure that the testing is aligned with the organization's risk appetite and compliance requirements. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3, Section 3.2.3.2, Page 137.

NEW QUESTION: 372

Optimized risk management is achieved when risk is reduced:

A. with strategic initiatives.

B. to meet risk appetite.

C. within resource availability.

D. below risk appetite.

Answer: (SHOW ANSWER)

Optimized risk management is achieved when risk is reduced to meet risk appetite, which is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk appetite reflects the strategic goals and priorities of the organization, as well as its risk culture and tolerance. Reducing risk with strategic initiatives, within resource availability, or below risk appetite are all possible approaches, but they do not necessarily optimize risk management, as they may result in over- or under-investment in risk

mitigation, or misalignment with business objectives. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.2, page 47

NEW QUESTION: 373
Who is ULTIMATELY accountable for the confidentiality of data in the event of a data breach within a Software as a Service (SaaS) environment?
A. Vendor's information security officer
B. Customer's data privacy officer
C. Customer's data owner
D. Vendor's application owner
Answer: (SHOW ANSWER)
In a SaaS model, while the provider manages the infrastructure and application,data ownership and ultimate responsibilityfor its confidentiality remains with thecustomer's data owner, including due diligence and contractual safeguards.
Reference:CRISC Manual - Domain 1, Slide 202-204

NEW QUESTION: 374
Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?
A. Reviewing the organization's policies and procedures
B. Interviewing groups of key stakeholders
C. Circulating questionnaires to key internal stakeholders
D. Accepting IT personnel s view of business issues
Answer: (SHOW ANSWER)
The best approach for performing a business impact analysis (BIA) of a supply-chain management application is to interview groups of key stakeholders, as this allows the risk practitioner to obtain direct and detailed information on the business processes, dependencies, resources, and requirements that are supported by the application. The risk practitioner can also clarify any doubts, address any concerns, and validate any assumptions during the interviews. The BIA is a process of identifying and analyzing the potential effects of disruptive events on the critical business functions and objectives. The BIA helps to determine the recovery priorities, strategies, and targets for the business continuity plan. The other options are not the best approaches for performing a BIA, although they may be useful or complementary methods. Reviewing the organization's policies and procedures can provide some background and context for the BIA, but it may not reflect the current or accurate situation of the business processes and the application. Circulating questionnaires to key internal stakeholders can be a convenient and efficient way to collect some data for the BIA, but it may not capture the complexity and nuances of the business processes and the application. Accepting IT personnel's view of business issues can be biased and incomplete, as they may not have the full understanding or perspective of the business needs and expectations. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 58.

NEW QUESTION: 375

A compensating control is MOST appropriate when:
A. Management wants to increase the number of controls.
B. A vulnerability is identified.
C. Existing controls are inadequate.
D. A key control is already in place and operating effectively.
Answer: (SHOW ANSWER)
A compensating control addresses risk when the primary control cannot meet the required objectives due to practical constraints.
Reference:CRISC Manual - Domain 3, Slide 345

NEW QUESTION: 376
Which of the following is the PRIMARY purpose of a risk register?
A. To assign control ownership of risk
B. To provide a centralized view of risk
C. To identify opportunities to transfer risk
D. To mitigate organizational risk
Answer: (SHOW ANSWER)
According to ISACA, a risk register is a tool to record and track the identified risks, their ratings, responses, and status. The primary purpose of a risk register is to provide a centralized view of risk for the organization, as it enables the consolidation, communication, and reporting of risk information across different levels, units, and functions. A risk register can also support the risk management process, such as risk identification, assessment, treatment, monitoring, and review.
References:
*ISACA, Risk IT Framework, 2nd Edition, 2019, p. 761
*ISACA, Capability Maturity Model and Risk Register Integration: The Right Approach to Enterprise Governance2

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 377
A risk register BEST facilitates which of the following risk management functions?
A. Analyzing the organization's risk appetite
B. Influencing the risk culture of the organization
C. Reviewing relevant risk scenarios with stakeholders
D. Articulating senior management's intent

Answer: (SHOW ANSWER)

Purpose of a Risk Register:

A risk register consolidates all identified risks, their status, and mitigation actions in one place. It serves as a tool for tracking and managing risks systematically.

Facilitating Risk Management Functions:

By documenting risk scenarios, a risk register provides a comprehensive view of potential threats and their impact on the organization.

It enables effective communication and review of these scenarios with stakeholders, ensuring that all relevant parties are aware of and understand the risks.

Engaging Stakeholders:

Reviewing the risk register with stakeholders helps in validating the risks, assessing their impact, and determining appropriate responses.

It fosters collaboration and ensures that risk management activities are aligned with the stakeholders' expectations and the organization's objectives.

Comparing Other Functions:

Analyzing Risk Appetite:While important, this is not the primary function of a risk register.

Influencing Risk Culture:The risk register contributes to risk culture but is primarily a tracking and communication tool.

Articulating Senior Management's Intent:This is more related to policy and strategy documents, whereas the risk register is a practical tool for managing specific risks.

References:

The CRISC Review Manual highlights the role of the risk register in consolidating risk information and facilitating stakeholder engagement (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.6 Risk Register) .

NEW QUESTION: 378

Which of the following is the MOST important characteristic when designing a key risk indicator (KRI)?

A. It is linked to a key performance indicator (KPI)

B. It is linked to a key control indicator (KCI)

C. It contains an objective alert threshold

D. It aligns with industry benchmarks

Answer: (SHOW ANSWER)

For a KRI to be actionable and effective, it must haveobjective thresholds. These thresholds act as triggers for decision-making and allow for timely response before risk materializes.

Reference:CRISC Manual - Domain 4, Slide 384-386

NEW QUESTION: 379

When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

A. Before defining a framework

B. During the risk assessment

C. When evaluating risk response
D. When updating the risk register
Answer: (SHOW ANSWER)
The best time to evaluate current control effectiveness when implementing an IT risk management program is during the risk assessment, as it involves measuring and testing the performance and adequacy of the existing controls, and identifying any control gaps or deficiencies that may affect the risk level and response. Before defining a framework, when evaluating risk response, and when updating the risk register are not the best times, as they are more related to the design, selection, or reporting of the controls, respectively, rather than the evaluation of the control effectiveness. References = CRISC Review Manual, 7th Edition, page 154.

NEW QUESTION: 380
An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:
Freecram.net
A. identifying risk scenarios.
B. determining the risk strategy.
C. calculating impact and likelihood.
D. completing the controls catalog.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, the risk register is a tool that records the results of risk identification, analysis, evaluation, and treatment. The risk register should be populated as soon as possible in the risk management process, to capture and document the risks and their attributes. The best time for the risk practitioner to start populating the risk register is when identifying risk scenarios, as this is the first step in the risk identification process. Risk scenarios are hypothetical situations that describe the potential causes, impacts, and responses of a risk event. Identifying risk scenarios helps to generate a comprehensive and relevant list of risks that can be recorded in the risk register. References = CRISC Review Manual1, page 191,
206.

NEW QUESTION: 381
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:
A. resources to monitor backups
B. restoration monitoring reports
C. backup recovery requests
D. recurring restore failures
Answer: (SHOW ANSWER)
The number of recurring restore failures is the best key performance indicator (KPI) to measure the effectiveness of a backup process, as it helps to evaluate the reliability and quality of the backup data and the backup system. A backup process is a process of creating and storing copies of data or systems to enable recovery in case of data loss, corruption, or disaster. A restore process is a process of retrieving and restoring the backup data or systems to the original or alternative location or state. A restore failure is an

event that occurs when the restore process fails to complete successfully or correctly, due to various reasons, such as corrupted or missing backup data, incompatible or outdated backup system, or insufficient or unavailable resources. A recurring restore failure is a restore failure that happens repeatedly or frequently, indicating a persistent or systemic problem with the backup process.
The number of recurring restore failures helps to measure the effectiveness of the backup process by providing the following benefits:
* It indicates the extent and magnitude of the backup process performance and quality issues, and the impact and severity of the backup process failures on the data or system availability and integrity.
* It identifies and analyzes the root causes and contributing factors of the backup process failures, and the gaps or weaknesses in the backup process design, implementation, operation, or monitoring.
* It provides feedback and learning opportunities for the backup process improvement and enhancement, and guides the development and implementation of corrective or preventive actions.
* It communicates and reports the backup process status and results to the relevant stakeholders, and supports the alignment of the backup process with the organizational strategy and objectives.
The other options are not the best key performance indicators (KPIs) to measure the effectiveness of a backup process. The number of resources to monitor backups is a measure of the inputs or costs of the backup process, but it does not indicate the outputs or benefits of the backup process. The number of restoration monitoring reports is a measure of the documentation or communication of the backup process, but it does not reflect the actual or potential performance or quality of the backup process. The number of backup recovery requests is a measure of the demand or frequency of the backup process, but it does not evaluate the reliability or quality of the backup process. References = 12 Process KPIs to Monitor Process Performance in 2024 - AIMultiple, IT Risk Resources | ISACA, Mastering RTO and RPO in Backup Strategies: A Key to Data Recovery Success

NEW QUESTION: 382
A recently purchased IT application does not meet project requirements. Of the following, who is accountable for the potential impact?
A. Business analyst
B. IT project team
C. Project sponsor
D. IT project management office (PMO)
Answer: (SHOW ANSWER)

NEW QUESTION: 383
A risk practitioner is summarizing the results of a high-profile risk assessment sponsored by senior management. The BEST way to support risk-based decisions by senior management would be to:
A. map findings to objectives.
B. provide quantified detailed analysis
C. recommend risk tolerance thresholds.
D. quantify key risk indicators (KRIs).
Answer: (SHOW ANSWER)

The best way to support risk-based decisions by senior management would be to map findings to objectives, because this would help them understand how the identified risks affect theachievement of the organization's goals and priorities. Mapping findings to objectives would also help senior management evaluate the trade-offs between different risk responses and allocate resources accordingly. By linking risks to objectives, the risk practitioner can communicate the value and impact of risk management in a clear and relevant way. References = Risk IT Framework, ISACA, 2022, p. 17

NEW QUESTION: 384
Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?
A. impact due to failure of control
B. Frequency of failure of control
C. Contingency plan for residual risk
D. Cost-benefit analysis of automation
Answer: D (LEAVE A REPLY)
Automation of control monitoring is the application of technology to allow continuous or high-frequency, automated monitoring of controls to validate the effectiveness of controls designed to mitigate risk1. Automation of control monitoring can provide benefits such as increased test coverage, improved timeliness, reduced risk velocity, greater visibility, improved consistency, and the ability to identify trends23. However, automation of control monitoring also involves costs such as the acquisition, implementation, maintenance, and updating of the technology, as well as the training and support of the staff who use it45. Therefore, the primary consideration when assessing the automation of control monitoring is the cost-benefit analysis of automation, which compares the expected benefits and costs of automation and determines whether the benefits outweigh the costs or vice versa45.
The other options are not the primary consideration, but rather secondary or tertiary factors that may influence the decision to automate or not. For example, the impact due to failure of controland the frequency of failure of control are aspects of the risk assessment that may indicate the need for automation, but they do not provide the basis for evaluating the feasibility and desirability of automation45. Similarly, the contingency plan for residual risk is a component of the risk response that may include automation as a risk mitigation strategy, but it does not measure the effectiveness and efficiency of automation45. References =
2: A Practical Approach to Continuous Control Monitoring, ISACA Journal, Volume 2, 2015
3: Continuous Controls Monitoring: The Next Generation Of Controls Testing, Forbes Technology Council, June 2, 2022
1: Making Continuous Controls Monitoring Work for Everyone, ISACA Now Blog, June 13, 2022
4: Controls Automation - Monitoring vs. Operation - Part 3, Turnkey Consulting, July 29, 2021
5: What's Continuous Control Monitoring and Why Is It Important?, MetricStream Blog, October 15, 2019

NEW QUESTION: 385
Which of the following can be used to assign a monetary value to risk?
A. Annual loss expectancy (ALE)
B. Business impact analysis

C. Cost-benefit analysis
D. Inherent vulnerabilities
Answer: (SHOW ANSWER)
Annual loss expectancy (ALE) is a method to assign a monetary value to risk by multiplying the probability of a risk event by the potential loss associated with that event1. ALE can be used to compare the costs and benefits of different risk mitigation options and to determine the optimal level of investment in risk management2. Business impact analysis (BIA) is a process to identify and evaluate the potential effects of a disruption on the critical functions and processes of an organization3. BIA can help to forecast the impacts of a risk event, but it does not assign a monetary value to the risk itself. Cost-benefit analysis (CBA) is a technique to compare the costs and benefits of a project, decision, or action4. CBA can help to evaluate the feasibility and profitability of a risk mitigation option, but it does not assign a monetary value to the risk itself. Inherent vulnerabilities are the weaknesses or flaws in a system, process, or asset that expose it to potential threats5. Inherent vulnerabilities can increase the likelihood or impact of a risk event, but they do not assign a monetary value to the risk itself. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.2: Risk Analysis, pp. 77-81.

NEW QUESTION: 386
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?
A. Unsupported end-user applications
B. Incomplete end-user device inventory
C. Multiple end-user device models
D. Incompatible end-user devices
Answer: (SHOW ANSWER)

NEW QUESTION: 387
Which of the following is a risk practitioner's MOST important course of action when the level of risk has exceeded risk tolerance?
A. Facilitate a review of risk tolerance levels
B. Adjust the risk impact and likelihood scale
C. Revise key risk indicator (KRI) thresholds
D. Introduce the risk treatment process
Answer: (SHOW ANSWER)
When risk exceeds tolerance, the appropriate action is to engage the risk treatment process. This involves evaluating and implementing appropriate responses such as mitigation, transfer, or acceptance.
Reference:CRISC Manual - Domain 3: Risk Response, Slide 110

NEW QUESTION: 388
The MOST essential content to include in an IT risk awareness program is how to:
A. populate risk register entries and build a risk profile for management reporting.
B. prioritize IT-related actions by considering risk appetite and risk tolerance.
C. define the IT risk framework for the organization.

D. comply with the organization's IT risk and information security policies.

Answer: (SHOW ANSWER)

The most essential content to include in an IT risk awareness program is how to comply with the organization's IT risk and information security policies. This will help to ensure that the staff members are aware of their roles and responsibilities, and that they follow the best practices and standards to protect the organization's information assets and systems. Compliance with the IT risk and information security policies also helps to reduce the likelihood and impact of IT-related incidents and breaches, and to align the IT activities with the organization's objectives and strategies. Populating risk register entries, prioritizing IT-related actions, and defining the IT risk framework are important aspects of IT risk management, but they are not the most essential content to include in an IT risk awareness program. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.1.1.2, page 2291
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 646.

NEW QUESTION: 389

Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

A. Obtaining logs m an easily readable format

B. Providing accurate logs m a timely manner

C. Collecting logs from the entire set of IT systems

D. implementing an automated log analysis tool

Answer: (SHOW ANSWER)

The most important requirement for monitoring key risk indicators (KRIs) using log analysis is providing accurate logs in a timely manner, because this ensures that the risk data is reliable, relevant, and up-to-date. Logs are records of events or activities that occur in IT systems, such as network traffic, user actions, system errors, or security incidents. Log analysis is the process of reviewing and interpreting logs to identify and assess risks, such as performance issues, operational failures, compliance violations, or cyberattacks. By providing accurate logs in a timely manner, an organization can monitor the current status and trends of its KRIs, which are metrics that measure the level and impact of risks. Accurate logs mean that the logs are complete, consistent, and free of errors or anomalies that may distort the risk data. Timely logs mean that the logs are available as soon as possible after the events or activities occur, and that they are updated frequently to reflect the latest changes. Providing accurate logs in a timely manner can help an organization to detect and respond to risks promptly, and to support risk-based decision making and reporting. References = Risk IT Framework, ISACA, 2022, p. 22

NEW QUESTION: 390

An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss expectancy. Which of the following is the BEST risk response?

Freecram.net

A. Mitigate

B. Accept

C. Transfer
D. Avoid
Answer: (SHOW ANSWER)
The best risk response for an identified high probability risk scenario involving a critical, proprietary business function with an annualized cost of control higher than the annual loss expectancy is to accept the risk. Accepting the risk means acknowledging the risk but choosing not to take any specific action to address it. This strategy is suitable when the cost of implementing controls exceeds the potential loss, as in this scenario.
The organization recognizes the risk, but the cost-benefit analysis suggests that the potential loss is acceptable given the higher cost of control. The other options are not the best risk responses, as they may not be feasible, practical, or cost-effective in this scenario. Mitigating the risk means reducing the risk by implementing controls or measures to minimize its potential impact, but this would increase the cost of control, which is already higher than the annual loss expectancy. Transferring the risk means shifting the risk to another party, typically through insurance or contracts, but this may not be possible or advisable for a critical, proprietary business function, and it may also increase the overall cost burden. Avoiding the risk means eliminating the risk entirely by not engaging in the activity that poses the risk, but this may disrupt essential business operations and potentially result in other adverse consequences. References = CRISC Exam: Best Risk Response for High Probability Risk Scenario; Risk Response Plan in Project Management: Key Strategies & Tips; Chapter 19: Summarizing Risk Management Concepts

NEW QUESTION: 391
External penetration tests MUST include:
A. changes to target data to prove the attack was successful.
B. advance approval from system owners.
C. use of consultants to ensure completeness.
D. communications to users of the target systems.
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 392
Which strategy employed by risk management would BEST help to prevent internal fraud?
A. Require control owners to conduct an annual control certification.
B. Conduct regular internal and external audits on the systems supporting financial reporting.
C. Ensure segregation of duties are implemented within key systems or processes.

D. Require the information security officer to review unresolved incidents.

Answer: (SHOW ANSWER)

Ensuring segregation of duties are implemented within key systems or processes is the best strategy employed by risk management to prevent internal fraud, because it reduces the opportunity for a single person to manipulate or misuse the system or process for fraudulent purposes. Segregation of duties is a control that assigns different roles and responsibilities to different individuals, such that no one person can perform all the steps of a transaction or process. Requiring control owners to conduct an annual control certification, conducting regular internal and external audits on the systems supporting financial reporting, and requiring the information security officer to review unresolved incidents are all useful strategies to detect or deter internal fraud, but they are not the best strategy to prevent it, as they do not directly address the root cause of fraud. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.3.1, page 197

NEW QUESTION: 393

What is the BEST approach for determining the inherent risk of a scenario when the actual likelihood of the risk is unknown?

A. Use the severity rating to calculate risk.

B. Classify the risk scenario as low-probability.

C. Use the highest likelihood identified by risk management.

D. Rely on range-based estimates provided by subject-matter experts.

Answer: (SHOW ANSWER)

When likelihood is unknown, range-based estimates from subject-matter experts provideinformed and realistic insights into potential risk exposure. This approach helps approximate the inherent risk based on experience and expertise, supporting effective decision-making.

NEW QUESTION: 394

Which of the following is the PRIMARY objective of risk management?

A. To identify and analyze risk

B. To achieve business objectives

C. To identify threats and vulnerabilities

D. To minimize business disruptions

Answer: (SHOW ANSWER)

NEW QUESTION: 395

Which of the following activities should be performed FIRST when establishing IT risk management processes?

A. Collect data of past incidents and lessons learned.

B. Conduct a high-level risk assessment based on the nature of business.

C. Identify the risk appetite of the organization.

D. Assess the goals and culture of the organization.

Answer: (SHOW ANSWER)

According to the Guide to Implementing an IT Risk Management Framework, the first activity that should be performed when establishing IT risk management processes is to assess the goals and culture of the organization. This is because the goals and culture of the organization define the context and scope of the IT risk management process, and influence the risk appetite and tolerance of the organization. By assessing the goals and culture of the organization, the IT risk manager can align the IT risk management process with the organization's strategy, vision, mission, values, and objectives. The IT risk manager can also identify the key stakeholders, roles, and responsibilities involved in the IT risk management process, and ensure that they have the necessary skills, knowledge, and resources to perform their tasks effectively. Additionally, the IT risk manager can establish the communication and reporting mechanisms for the IT risk management process, and ensure that they are consistent with the organization's culture and expectations. References = Guide to Implementing an IT Risk Management Framework, An Overview of the Risk Management Process

NEW QUESTION: 396
Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?
A. IT management
B. Internal audit
C. Process owners
D. Senior management
Answer: (SHOW ANSWER)
Process owners are the best suited to help a risk practitioner understand the impact of IT-related events on business objectives, as they have the responsibility and authority over the design, execution, and performance of business processes. Process owners are also accountable for the risks and controls associated with their processes, and they can provide valuable input and feedback on the likelihood and impact of IT-related events on the process outcomes and objectives.
The other options are not the best suited to help a risk practitioner understand the impact of IT-related events on business objectives. IT management is responsible for the delivery and support of IT services and solutions, but they may not have the full visibility or understanding of the business objectives and processes. Internal audit is responsible for providing independent and objective assurance and consulting services on the effectiveness and efficiency of governance, risk management, and control processes, but they may not have the direct involvement or influence on the business objectives and processes. Senior management is responsible for setting the strategic direction and objectives of the organization, but they may not have the detailed knowledge or experience of the business processes and their risks and controls. References = IT Risk Manager: Skills and Roles & Responsibilities, IT Risk Resources | ISACA, Managing information technology risk | Business Queensland

NEW QUESTION: 397
Which of the following is the PRIMARY objective of risk management?
A. Identify and analyze risk.
B. Achieve business objectives
C. Minimi2e business disruptions.

D. Identify threats and vulnerabilities.

Answer: (SHOW ANSWER)

The primary objective of risk management is to achieve business objectives, as risk management involves identifying, assessing, responding, and monitoring the risks that may affect the desired outcomes and performance of the organization, and aligning them with the risk tolerance and appetite of the organization. Identifying and analyzing risk, minimizing business disruptions, andidentifying threats and vulnerabilities are not the primary objectives, as they are more related to the process, outcome, or source of risk management, respectively, rather than the purpose or value of risk management. References = CRISC Review Manual, 7th Edition, page 99.

NEW QUESTION: 398

When performing a risk assessment of a new service to support a core business process, which of the following should be done FIRST to ensure continuity of operations?

A. Define metrics for restoring availability.

B. Identify conditions that may cause disruptions.

C. Review incident response procedures.

D. Evaluate the probability of risk events.

Answer: (SHOW ANSWER)

When performing a risk assessment of a new service to support a core business process, the first step is to identify the conditions that may cause disruptions to the service or the process. This involves identifying the sources and causes of potential risk events, such as natural disasters, cyberattacks, human errors, equipment failures, power outages, etc. that may affect the availability, integrity, or confidentiality of the service or the process. By identifying the conditions that may cause disruptions, the risk practitioner can then analyze the probability and impact of the risk events, evaluate the risk exposure, and determine the appropriate risk responses to ensure the continuity of operations. References = CRISC Review Manual, 7th Edition, page 66.

NEW QUESTION: 399

Which of the following is the BEST way to identify changes in the risk profile of an organization?

A. Monitor key risk indicators (KRIs).

B. Monitor key performance indicators (KPIs).

C. Interview the risk owner.

D. Conduct a gap analysis

Answer: (SHOW ANSWER)

The best way to identify changes in the risk profile of an organization is to monitor key risk indicators (KRIs), which are metrics that provide information on the level of exposure to a given operational risk1. KRIs can help to monitor the changes in risk levels over time, identify emerging risks, and trigger risk response actions when the risk exceeds the acceptable thresholds2. KRIs can also help to align the risk management strategy with the business objectives and context. The other options are not the best ways to identify changes in the risk profile of an organization, as they do not provide the same level of insight and guidance as KRIs.

Monitoring key performance indicators (KPIs) may show the results or outcomes of the business processes, but not the risks or uncertainties that affect them. Interviewing the risk owner may provide some subjective or qualitative information on the risk perception or attitude, but not the objective or quantitative data on the risk exposure or impact. Conducting a gap analysis may show the difference between the current and desired state of the organization, but not the causes or sources of the risk. References = Key Risk Indicators; Key Risk Indicators: A Practical Guide

NEW QUESTION: 400

A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

Freecram.net

A. Internal audit
B. Control owner
C. Senior management
D. Risk manager
Answer: (SHOW ANSWER)

A purchase order approval process is a set of procedures that companies use to authorize the purchase of goods or services from suppliers1. This process typically involves multiple levels of approvals, ensuring that purchases are compliant with company regulations and policies, and within budget limitations1. Sometimes, a department may be granted an exception to bypass the existing approval process for purchase orders, for example, due to urgency, emergency, or special circumstances2. However, such exceptions should not compromise the effectiveness and integrity of the purchase order approval process, and should be properly documented and justified2. Therefore, the risk practitioner should verify that the exception has been approved by senior management, as they are ultimately responsible for setting and overseeing the purchase order approval process, and for ensuring that the exceptions are reasonable and aligned with the company's objectives and risk appetite3. Internal audit is not the correct answer, as they are not involved in approving the purchase order approval process or its exceptions. Internal audit's role is to provide independent assurance and advice on the adequacy and effectiveness of the purchase order approval process and its controls, and to report any issues or recommendations for improvement4. Control owner is not the correct answer, as they are not involved in approving the purchase order approval process or its exceptions. Control owner's role is to design, implement, and operate the controls that support the purchase order approval process, and to monitor and report on the performance and compliance of the controls5. Risk manager is not the correct answer, as they are not involved in approving the purchase order approval process or its exceptions. Risk manager's role is to identify, assess, and mitigate the risks associated with the purchase order approval process, and to communicate and report on the risk status and issues6. References = 1: A Step-by-Step Guide to a Purchase Order Approval Process2: Purchase Order Exceptions | Fordham3: Purchase Order (PO) Approval Process and Approval Workflow - ProcureDesk4: IT Risk Resources | ISACA5: CRISC Resources [updated 2021] | Infosec6: Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.

NEW QUESTION: 401

Which of the following risk activities is BEST facilitated by enterprise architecture (EA)?

A. Customizing incident response plans for each business unit
B. Aligning business unit risk responses to organizational priorities
C. Adjusting business unit risk tolerances
D. Determining attack likelihood per business unit
Answer: (SHOW ANSWER)

NEW QUESTION: 402
During a data loss incident, which role in the RACI chart would be aligned to the risk practitioner?
A. Consulted
B. Responsible
C. Accountable
D. Informed
Answer: (SHOW ANSWER)

NEW QUESTION: 403
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?
A. Unknown vulnerabilities
B. Legacy technology systems
C. Network isolation
D. Overlapping threats
Answer: (SHOW ANSWER)
Architecture is the design and structure of a system or a process, such as an IT system or a business process.
Architecture documentation is the document that describes and explains the architecture, such as its components, functions, relationships, requirements, constraints, orstandards. Architecture documentation can help to understand, communicate, and improve the system or the process1.
An environment that lacks documentation of the architecture faces a great risk of unknown vulnerabilities, which are the weaknesses or flaws in the system or the process that could be exploited by threats or attackers, but are not identified or addressed by the organization. Unknown vulnerabilities can pose a serious risk to the organization, because they can:
Compromise the confidentiality, integrity, and availability of the system or the process, and the information or resources that it handles or supports Cause financial, operational, reputational, or legal damages or losses to the organization, such as data breaches, fraud, errors, delays, or fines Remain undetected or unresolved for a long time, and increase the exposure or impact of the risk over time Require more resources or efforts to mitigate or recover from the risk, and reduce the efficiency or effectiveness of the risk management process23 Lack of documentation of the architecture can increase the risk of unknown vulnerabilities, because it can:
Prevent or hinder the identification and assessment of the vulnerabilities, and the evaluation and prioritization of the risks Impede or delay the implementation and enforcement of the controls or safeguards to prevent or reduce the vulnerabilities, and the monitoring and reporting of the risk status and progress Obstruct or limit

the communication and coordination among the stakeholders, and the awareness and accountability of the risk owners and users Restrict or hamper the review and improvement of the system or the process, and the learning and feedback of the risk management4 The other options are not the greatest risks associated with an environment that lacks documentation of the architecture, but rather some of the possible causes or consequences of it.Legacy technology systems are outdated or obsolete systems that are still in use by the organization, but are no longer supported or maintained by the vendors or developers. Legacy technology systems can be a cause of lack of documentation of the architecture, as they may have been developed or acquired without proper documentation, or the documentation may have been lost or discarded over time. Network isolation is the separation or segregation of a network or a system from other networks or systems, either physically or logically, to prevent or limit the access or communication between them. Network isolation can be a consequence of lack of documentation of the architecture, as it may result from the inability or difficulty to integrate or connect the system or the process with other systems or processes. Overlapping threats are threats that affect more than one system or process, or have similar or related sources or causes, such as natural disasters, cyberattacks, or human errors.
Overlapping threats can be a consequence of lack of documentation of the architecture, as they may arise from the lack of understanding or coordination of the system or the process with other systems or processes.
References = Architecture Documentation - ISACA Vulnerability - ISACA The Risks of Not Having a Vulnerability Management Program The Importance of Architecture Documentation - ISACA
[The Risk of Poor Document Control - ComplianceBridge]
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 404
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:
A. process flow.
B. business impact analysis (BIA).
C. service level agreement (SLA).
D. system architecture.
Answer: (SHOW ANSWER)
The most helpful information to review when determining a system's criticality is the associated business impact analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to the organization's critical business functions and processes. A BIA can help to determine the system's criticality by assessing its impact on the organization's objectives, performance, and value. Process flow, service level agreement (SLA), and system architecture are other possible information sources, but they are not as helpful as the BIA. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 4; CRISC Review Manual, 6th Edition, page 153.

NEW QUESTION: 405
Which of the following contributes MOST to the effective implementation of risk responses?
A. Clear understanding of the risk
B. Comparable industry risk trends
C. Appropriate resources

D. Detailed standards and procedures

Answer: (SHOW ANSWER)

Appropriate resources contribute most to the effective implementation of risk responses. Resources include people, time, money, equipment, and materials that are needed to execute the risk responses. Without appropriate resources, the risk responses may not be implemented properly, timely, or efficiently, and may not achieve the desired outcomes. The other options are not as important as appropriate resources, as they are related to the understanding, comparison, or documentation of the risk responses, which are less critical than the execution of the risk responses. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 406

After undertaking a risk assessment of a production system, the MOST appropriate action is for the risk manager to:

A. recommend a program that minimizes the concerns of that production system.

B. inform the development team of the concerns, and together formulate risk reduction measures.

C. inform the process owner of the concerns and propose measures to reduce them

D. inform the IT manager of the concerns and propose measures to reduce them.

Answer: (SHOW ANSWER)

* A risk assessment of a production system is a process of identifying, analyzing, evaluating, and treating the risks that may affect the performance, quality, or safety of the production system, which is a system that transforms inputs into outputs using various resources, processes, and technologies12.
* The most appropriate action for the risk manager to take after undertaking a risk assessment of a production system is to inform the process owner of the concerns and propose measures to reduce them, which is a process of communicating and consulting with the person who is responsible for the design, operation, and improvement of the production system, and suggesting possible risk responses that can prevent, mitigate, transfer, or accept the risks34.
* This action is the most appropriate because it ensures the involvement and collaboration of the process owner, who has the authority and accountability to implement and monitor the risk responses, and who can provide feedback and input on the feasibility and effectiveness of the proposed measures34.
* This action is also the most appropriate because it supports the risk management process and objectives, which are to identify and address the risks that may affect the achievement of the organization's goals and the delivery of value to the stakeholders34.
* The other options are not the most appropriate actions, but rather possible alternatives or supplements that may have some limitations or drawbacks. For example:
* Recommending a program that minimizes the concerns of the production system is an action that involves designing and planning a set of coordinated and interrelated activities and tasks that aim to reduce the likelihood or impact of the risks34. However, this action is not the most appropriate because it does not involve the process owner, who is the key stakeholder and decision maker for the production system, and who may have different views or preferences on the risk responses34.
* Informing the development team of the concerns, and together formulating risk reduction measures is an action that involves communicating and consulting with the group of people who are responsible for creating,

testing, and deploying the products or services that are produced by the production system, and jointly developing possible risk responses34. However, this action is not the most appropriate because it does not involve the process owner, who is the primary owner and user of the production system, and who may have different needs or expectations on the risk responses34.
* Informing the IT manager of the concerns and proposing measures to reduce them is an action that involves communicating and consulting with the person who is responsible for managing and overseeing the IT resources, processes, and systems that support the production system, and suggesting possible risk responses34. However, this action is not the most appropriate because it does not involve the process owner, who is the main stakeholder and beneficiary of the production system, and who may have different requirements or constraints on the risk responses34. References =
* 1: Risk Assessment for the Production Process1
* 2: Risk Assessment for Industrial Equipment2
* 3: Risk IT Framework, ISACA, 2009
* 4: IT Risk Management Framework, University of Toronto, 2017

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 407
Which of the following is the MOST important consideration when implementing ethical remote work monitoring?
A. Monitoring is only conducted between official hours of business
B. Employees are informed of how they are bong monitored
C. Reporting on nonproductive employees is sent to management on a scheduled basis
D. Multiple data monitoring sources are integrated into security incident response procedures
Answer: (SHOW ANSWER)
The most important consideration when implementing ethical remote work monitoring is to inform the employees of how they are being monitored, because this respects their privacy rights and expectations, and ensures their consent and compliance with the monitoring policy. Informing the employees of how they are being monitored also helps to build trust and transparency between the employer and the employees, and reduces the potential legal or ethical issues that may arise from the monitoring activities. The other options are not the most important considerations, although they may also be relevant for ethical remote work monitoring.
Monitoring only during official hours of business, reporting on nonproductive employees to management, and integrating multiple data monitoring sources into security incident response procedures are examples of

operational or technical aspects of remote work monitoring, not ethical aspects. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 408
Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?
A. Hire consultants specializing m the new technology.
B. Review existing risk mitigation controls.
C. Conduct a gap analysis.
D. Perform a risk assessment.
Answer: (SHOW ANSWER)
A risk assessment is a process of measuring and comparing the likelihood and impact of various risk scenarios, and prioritizing them based on their significance and urgency. A risk assessmentcan help the organization to understand and document the risks that may affect its objectives and operations, and to support the decision making and planning for the risk management.
Performing a risk assessment would be the most helpful to understand the impact of a new technology system on an organization's current risk profile, because it can help the organization to address the following questions:
What are the potential benefits and challenges of implementing the new technology system, and how do they align with the organization's objectives and needs?
What are the existing or emerging risks that may affect the new technology system, and how do they relate to the organization's current risk profile?
How likely and severe are the risks that may affect the new technology system, and what are the possible consequences or impacts for the organization and its stakeholders?
How can the risks that may affect the new technology system be mitigated or prevented, and what are the available or feasible options or solutions?
Performing a risk assessment can help the organization to understand the impact of the new technology system on its current risk profile by providing the following benefits:
It can enable the comparison and evaluation of the current and desired state and performance of the organization's risk management function, and to identify and quantify the gaps or opportunities for improvement.
It can provide useful references and benchmarks for the alignment and integration of the new technology system with the organization's risk management function, and for the compliance with the organization's risk policies and standards.
It can support the implementation and monitoring of the new technology system, and for the allocation and optimization of the resources, time, and budget for the new technology system.
The other options are not the most helpful to understand the impact of a new technology system on an organization's current risk profile, because they do not provide the same level of detail and insight that performing a risk assessment provides, and they may not be specific or applicable to the organization's objectives and needs.

Hiring consultants specializing in the new technology means engaging or contracting external experts or professionals that have the skills and knowledge on the new technology system, and that can provide advice or guidance on the implementation and management of the new technology system. Hiring consultants specializing in the new technology can help the organization to enhance its competence and performance on the new technology system, but it is not the most helpful, because it does not measure and compare the likelihood and impact of the risks that may affect the new technology system, and it may not be relevant or appropriate for the organization's current risk profile.
Reviewing existing risk mitigation controls means examining and evaluating the adequacy and effectiveness of the controls or countermeasures that are intended to reduce or eliminate the risksthat may affect the organization's objectives and operations. Reviewing existing risk mitigation controls can help the organization to improve and optimize its risk management function, but it is not the most helpful, because it does not identify and prioritize the risks that may affect the newtechnology system, and it may not cover all the relevant or significant risks that may affect the new technology system.
Conducting a gap analysis means comparing and contrasting the current and desired state and performance of the organization's objectives and operations, and identifying and quantifying the gaps or differences that need to be addressed or corrected. Conducting a gap analysis can help the organization to identify and document its improvement needs and opportunities, but it is not the most helpful, because it does not measure and compare the likelihood and impact of the risks that may affect the new technology system, and it may not be aligned or integrated with the organization's current risk profile. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 208 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 409
Establishing and organizational code of conduct is an example of which type of control?
A. Preventive
B. Directive
C. Detective
D. Compensating
Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), establishing an organizational code of conduct is an example of a directive control, which is a type of control that guides or steers the behavior of individuals or processes to achieve desired outcomes. A directive control aims to influence or encourage compliance with the organization's policies, standards, procedures, and guidelines. A directive control can also communicate the organization's values, ethics, and expectations to its stakeholders. A directive control can take various forms, such as:
* Codes of conduct or ethics
* Policies or manuals
* Training or awareness programs
* Job descriptions or roles and responsibilities

* Performance appraisals or incentives
* Supervision or oversight
References = CRISC Review Manual (Digital Version), Chapter 2: IT Risk Assessment, Section 2.4: IT Risk Scenarios, pp. 105-1061

NEW QUESTION: 410
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?
Freecram.net
A. Obtain industry benchmarks related to the specific risk.
B. Provide justification for the lower risk rating.
C. Notify the business at the next risk briefing.
D. Reopen the risk issue and complete a full assessment.
Answer: (SHOW ANSWER)
The best course of action in responding to the internal audit inquiry is to provide justification for the lower risk rating. This would demonstrate that the risk record was updated based on a valid and documented rationale, such as changes in the risk environment, risk drivers, risk indicators, or risk responses. Providing justification would also help to maintain the transparency and accountability of the risk management process, and ensure that the internal audit is satisfied with the risk assessment outcome. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.3, page 184.

NEW QUESTION: 411
A contract associated with a cloud service provider MUST include:
A. ownership of responsibilities.
B. a business recovery plan.
C. provision for source code escrow.
D. the providers financial statements.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), a contract associated with a cloud service provider must include ownership of responsibilities, as this defines the roles and obligations of both the cloud provider and the customer in relation to the cloud services. The contract should specify who is responsible for:
* Service delivery and performance
* Data security and privacy
* Compliance with regulations and standards
* Incident management and reporting
* Business continuity and disaster recovery
* Change management and configuration control
* Intellectual property rights and licensing
* Termination and data egress
The contract should also include service level agreements (SLAs) that measure and monitor the quality and availability of the cloud services, as well as remedies and penalties for non-compliance. The contract should

also address pricing and payment terms, dispute resolution mechanisms, and liability and indemnification clauses.
References = CRISC Review Manual (Digital Version), Chapter 3: IT Risk Response, Section 3.3: Risk Response Options, pp. 173-1741

NEW QUESTION: 412
An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?
A. Acceptance
B. Transfer
C. Mitigation
D. Avoidance
Answer: B (LEAVE A REPLY)
According to the ERM - Step 3 - Risk Treatment article, risk transfer is a risk treatment option that involves passing ownership and/or liability of a risk to a third party, such as an insurance company, a contractor, or a supplier. Risk transfer is usually adopted when the organization does not have the capability or the resources to manage the risk internally, or when the cost of transferring the risk is lower than the cost of retaining the risk. In this case, the organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. This means that the organization has transferred the risk of non-compliance to the service provider, who is now responsible for ensuring that the lease payment process meets the regulatory requirements. Therefore, the answer is B. Transfer. References = ERM - Step 3 - Risk Treatment

NEW QUESTION: 413
The MAIN purpose of selecting a risk response is to.
A. ensure compliance with local regulatory requirements
B. demonstrate the effectiveness of risk management practices.
C. ensure organizational awareness of the risk level
D. mitigate the residual risk to be within tolerance
Answer: (SHOW ANSWER)
The main purpose of selecting a risk response is to mitigate the residual risk to be within tolerance. Residual risk is the risk that remains after applying a risk response. Risk tolerance is the amount and type of risk that an organization is willing to accept in order to achieve its objectives. Risk response is the process of selecting and implementing actions to address risk. The goal of risk response is to reduce the residual risk to a level that is acceptable to the organization and its stakeholders. The other options are not the main purpose of selecting a risk response, although they may be secondary benefits or outcomes. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.1, page 4-23.

NEW QUESTION: 414
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?
A. involve IT leadership in the policy development process

B. Require business users to sign acknowledgment of the poises
C. involve business owners in the pokey development process
D. Provide policy owners with greater enforcement authority
Answer: (SHOW ANSWER)
To ensure that new IT policies address the enterprise's requirements, it is important to involve the business owners who are the primary stakeholders of the IT services and processes. Business owners can provide valuable input on the business objectives, risks, and expectations that the IT policies should align with and support. By involving business owners in the policy development process, the IT policies will be more relevant, realistic, and acceptable to the business units. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.3: IT Risk Scenarios, page 23.

NEW QUESTION: 415
Which of the following is the MOST important reason to communicate control effectiveness to senior management?
A. To demonstrate alignment with industry best practices
B. To assure management that control ownership is assigned
C. To ensure management understands the current risk status
D. To align risk management with strategic objectives
Answer: (SHOW ANSWER)
According to the ISACA Risk and Information Systems Control study guide and handbook, the most important reason to communicate control effectiveness to senior management is to ensure management understands the current risk status. Control effectiveness is a measure of how well a control reduces the likelihood or impact of a risk event. By communicating control effectiveness, risk managers can provide management with relevant and timely information about the residual risk level, the risk appetite and tolerance, and the potential gaps or weaknesses in the control environment. This can help management make informed decisions about risk response strategies, resource allocation, and risk oversight12
1: ISACA Risk and Information Systems Control Study Guide, 4th Edition, page 33 2: ISACA Risk and Information Systems Control Handbook, 1st Edition, page 25

NEW QUESTION: 416
Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?
A. Network monitoring infrastructure
B. Centralized vulnerability management
C. Incident management process
D. Centralized log management
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, centralized log management is the best way to assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network, because it enables the collection, correlation, analysis, and retention of log data from various sources. Centralized log management can provide a comprehensive and consistent view of the

activities and transactions that occurred before, during, and after the incident, and can facilitate the identification of the root cause, impact, and scope of the incident. The other options are not the best ways to assist in reconstructing the sequence of events, because they do not provide the same level of detail and accuracy as centralized log management. Network monitoring infrastructure is a tool that helps to monitor the performance and availability of the network, but it does not capture the log data from the IT systems. Centralized vulnerability management is a process that helps to identify and remediate the vulnerabilities in the IT systems, but it does not record the events and transactions that occurred on the systems. Incident management process is a process that helps to respond to and resolve the incidents, but it does not provide the log data from the IT systems. References = CRISC Review Manual, 7th Edition, Chapter 5, Section 5.3.2, page 263.

NEW QUESTION: 417
When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported to:
A. Assess generic risk scenarios with business users.
B. Validate the generic risk scenarios for relevance.
C. Select the maximum possible risk scenarios from the list.
D. Identify common threats causing generic risk scenarios
Answer: (SHOW ANSWER)
The most important step when developing risk scenarios using a list of generic scenarios based on industry best practices is to validate the generic risk scenarios for relevance. The generic risk scenarios may not be applicable or suitable for the specific context, objectives, and environment of the organization. Therefore, the risk practitioner should validate the relevance of the generic risk scenarios by comparing them with the organization's risk profile, risk appetite, and risk criteria. Assessing generic risk scenarios with business users, selecting the maximum possible risk scenarios from the list, and identifying common threats causing generic risk scenarios are other steps that may be useful, but they are not as important as validating the relevance of the generic risk scenarios. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 12; CRISC Review Manual, 6th Edition, page 215.

NEW QUESTION: 418
Recent penetration testing of an organization's software has identified many different types of security risks. Which of the following is the MOST likely root cause for the identified risk?
A. SIEM software is producing faulty alerts.
B. Threat modeling was not utilized in the software design process.
C. The configuration management process is not applied consistently during development.
D. An identity and access management (IAM) tool has not been properly integrated into the software.
Answer: (SHOW ANSWER)
Failure to utilize threat modeling during the design phase results in overlooked vulnerabilities. This highlights the importance ofProactive Threat Identificationin secure software development practices.

NEW QUESTION: 419
Of the following, who should be responsible for determining the inherent risk rating of an application?
A. Application owner
B. Senior management
C. Risk practitioner
D. Business process owner
Answer: (SHOW ANSWER)
Inherent risk rating is a measure of the natural level of risk that is part of an application, before any controls are applied1. Inherent risk rating helps to identify and prioritize the applications that pose the highest risk to the organization and require the most attention and resources for risk management2. The responsibility for determining the inherent risk rating of an application should belong to the risk practitioner, as they have the expertise and knowledge to perform a comprehensive and consistent risk assessment of the application, using a standard methodology and criteria3. The risk practitioner should also communicate and report the inherent risk rating of the application to the relevant stakeholders, such as the application owner, senior management, and business process owner, and provide recommendations for risk mitigation4. The application owner, senior management, and business process owner are not the best choices for determining the inherent risk rating of an application, as they may not have the same level of skill and objectivity as the risk practitioner. The application owner is the person who has the authority and accountability for the application and its performance5. The application owner may be involved in providing input and feedback to the risk practitioner during the risk assessment process, but they may not be able to assess the inherent risk rating of the application independently and impartially, as they may have a vested interest in the application's success and reputation6. Senior management is the group of executives who set the strategic direction and objectives of the organization and oversee its performance7. Senior management may be involved in approving and endorsing the risk assessment process and its results, but they may not be able to assess the inherent risk rating of the application in detail and depth, as they may have a broader and higher-level perspective of the organization's risk profile and priorities8. The business process owner is the person who has the authority and accountability for a business process that is supported or enabled by the application. The business process owner may be involved in providing input and feedback to the risk practitioner during the risk assessment process, but they may not be able to assess the inherent risk rating of the application accurately and comprehensively, as they may have a limited and specific view of the application's functionality and value. References = 2: Introduction toapplication risk rating & assessment | Infosec3: Application Security Risk: Assessment and Modeling - ISACA4: Risk and Information Systems Control Study Manual, Chapter 4:
Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.1: Inherent Risk Rating - Shared Assessments - Third Party Risk Management5: [Application Owner - Gartner IT Glossary] 6: Perform Inherent Risk Analysis - Oracle7: [Senior Management - Definition, Roles and Responsibilities] 8: Rating Inherent and Residual Risk - Barn Owl : [Business Process Owner - Gartner IT Glossary] : [Business Process Owner - Roles and Responsibilities]

NEW QUESTION: 420

When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

Freecram.net

A. Sharing company information on social media

B. Sharing personal information on social media

C. Using social media to maintain contact with business associates

D. Using social media for personal purposes during working hours

Answer: A (LEAVE A REPLY)

The most important concern to address when formulating a social media policy to address information leakage is sharing company information on social media. Information leakage is the unauthorized or unintentional disclosure of confidential or sensitive information to unauthorized parties. Social media is a platform that enables the users to create and share content, such as text, images, videos, or links, with other users or the public. Sharing company information on social media is the most important concern, as it could expose the company's trade secrets, intellectual property, customer data, financial data, or strategic plans to competitors, hackers, or regulators. Sharing company information on social media could also damage the company's reputation, trust, or credibility, and result in legal or regulatory penalties, fines, or lawsuits. Therefore, a social media policy should clearly define what constitutes company information, and what are the rules and guidelines for sharing or not sharing company information on social media. A social media policy should also specify the roles and responsibilities of the employees, managers, and the social media team, and the consequences and sanctions for violating the policy. Sharing personal information on social media, using social media to maintain contact with business associates, and using social media for personal purposes during working hours are not as important as sharing company information on social media, as they do not directly involve the leakage of company information, and they may not have significant impact or risk on the company. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217

NEW QUESTION: 421

WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

A. Enforce sanctions for noncompliance with security procedures.

B. Conduct organization-w>de phishing simulations.

C. Require training on the data handling policy.

D. Require regular testing of the data breach response plan.

Answer: (SHOW ANSWER)

The most effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage is to require training on the data handling policy, as it educates the employees on the importance, requirements, and procedures of data protection, and enhances their knowledge and skills to prevent, detect, and respond to data leakage incidents. Enforcing sanctions for noncompliance with security procedures, conducting organization-wide phishing simulations, and requiring regular testing of the data breach response plan are not the most effective ways, as they are more related to the enforcement, evaluation, or improvement of the data security, respectively, rather than the promotion of the data security awareness. References = CRISC Review Manual, 7th Edition, page 155.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 422
Which of the following is MOST useful when communicating risk to management?
A. Risk policy
B. Audit report
C. Risk map
D. Maturity model
Answer: (SHOW ANSWER)
A risk map is a visual tool that helps to communicate risk to management by showing the likelihood and impact of different risks on a matrix1. A risk map can help to:
Identify the most critical risks that need immediate attention or action Compare and prioritize risks based on their severity and probability Align risk management strategies with the organization's risk appetite and tolerance Communicate risk information in a clear and concise way that is easy to understand and interpret2
References = Risk and Information Systems Control Study Manual, Chapter 5: Risk Assessment Process3

NEW QUESTION: 423
Which of the following is the BEST method to maintain a common view of IT risk within an organization?
A. Collecting data for IT risk assessment
B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis
Answer: (SHOW ANSWER)
The best method to maintain a common view of IT risk within an organization is to establish and communicate the IT risk profile. An IT risk profile is a document that summarizes the key IT risks that the organization faces or accepts, and their likelihood, impact, and priority. An IT risk profile helps to identify and prioritize the most critical or relevant IT risks, and to align them with the organization's objectives, strategy, and risk appetite. Establishing and communicating the IT risk profile is the best method to maintain a common view of IT risk, because it helps to create a shared understanding and awareness of the IT risks among the organization's stakeholders, such as the board, management, business units, and IT functions. Establishing and communicating the IT risk profile also helps to facilitate the IT risk decision-making and reporting processes, and to monitor and control the IT risk performance and improvement. Theother options are not the best method to maintain a common view of IT risk, although they may be part of or derived from the IT risk profile. Collecting data for IT risk assessment, utilizing a balanced scorecard, and performing and publishing an IT risk analysis are all activities that can help to support or update the IT risk profile, but they

are not the best method to maintain a common view of IT risk. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.1, page 1-15.

NEW QUESTION: 424
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager to exclude an in-scope system from a risk assessment?
A. Postpone the risk assessment.
B. Facilitate the exception process.
C. Accept the manager's request.
D. Reject the manager's request.
Answer: (SHOW ANSWER)
Facilitating the exception process ensures that any deviations from the standard risk assessment procedures are formally documented, reviewed, and approved by appropriate governance bodies. This approach maintains the integrity of the risk management process while addressing the business unit manager's concerns.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 2: IT Risk Assessment, Section: Risk Assessment Process.

NEW QUESTION: 425
Which of the following is the PRIMARY objective for automating controls?
A. Reducing the need for audit reviews
B. Facilitating continuous control monitoring
C. Improving control process efficiency
D. Complying with functional requirements
Answer: (SHOW ANSWER)
The primary objective of automating controls is to facilitate continuous control monitoring. Automation enables real-time or near-real-time oversight of control activities, allowing for prompt detection and response to control failures or anomalies. This continuous monitoring enhances the organization's ability to maintain compliance and manage risks effectively.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Control Monitoring and Automation.

NEW QUESTION: 426
Which of the following activities should only be performed by the third line of defense?
A. Operating controls for risk mitigation
B. Testing the effectiveness and efficiency of internal controls
C. Providing assurance on risk management processes
D. Recommending risk treatment options
Answer: (SHOW ANSWER)
Providing assurance on risk management processes is the activity that should only be performed by the third line of defense, because it is the role and responsibility of the independent and objective assurance function,

such as internal audit or external audit, to evaluate and report on the effectiveness and efficiency of the risk management processes and controls. The third line of defense is the last layer of the three lines of defense model, which is a framework that defines the roles and responsibilities of different functions and levels within the organization for risk management and control. The first line of defense is the operational management and staff, who are responsible for identifying, assessing, and managing the risks and controls within their areas of responsibility. The second line of defense is the oversight and support functions, such as risk management, compliance, or legal, who are responsible for establishing and monitoring the risk policies, standards, and frameworks, and providing guidance and advice to the first line of defense. The third line of defense is the assurance function, who are responsible for providing independent and objective assurance on the adequacy and effectiveness of the risk management processes and controls, and reporting to the senior management and the board of directors. Operating controls for risk mitigation, testing the effectiveness and efficiency of internal controls, and recommending risk treatment options are all activities that can be performed by the first or second line of defense, but not by the third line of defense, as they are not part of the assurance function.
References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.4.1, page 59

NEW QUESTION: 427
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:
A. business process objectives have been met.
B. control adheres to regulatory standards.
C. residual risk objectives have been achieved.
D. control process is designed effectively.
Answer: (SHOW ANSWER)
When reviewing a report on the performance of control processes, it is most important to verify whether the residual risk objectives have been achieved, as this indicates the extent to which the control processes have reduced the risk to an acceptable level. Residual risk is the risk that remains after the implementation of controls, and it should be aligned with the risk appetite and tolerance of the enterprise. Business process objectives, regulatory standards, and control process design are not the most important factors to verify,as they do not directly measure the effectiveness and efficiency of the control processes in managing the risk.
References = CRISC Practice Quiz and Exam Prep; CRISC: Certified in Risk & Information Systems Control Sample Questions, question 209.

NEW QUESTION: 428
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?
A. Ensuring processes are documented to enable effective control execution
B. Ensuring regular risk messaging is Included in business communications from leadership
C. Ensuring schedules and deadlines for control-related deliverables are strictly monitored
D. Ensuring performance metrics balance business goals with risk appetite
Answer: (SHOW ANSWER)

The most important thing for mitigating ethical risk when establishing accountability for control ownership is to ensure that the performance metrics balance business goals with risk appetite. Performance metrics are the measures that evaluate the achievement of the objectives or the performance of the processes or controls.
Business goals are the desired or expected outcomes or results of the business activities or processes. Risk appetite is the amount and type of risk that the organization is willing and able to take. Ethical risk is the risk that arises from the violation or breach of the ethical principles or standards of the organization or the profession. To mitigate ethical risk, the performance metrics should balance business goals with risk appetite, meaning that they should not encourage or reward excessive or inappropriate risk-taking or unethical behavior, but rather promote and support responsible and ethical risk management and decision making. The other options are not as important as ensuring performance metrics balance business goals with risk appetite, as they are related to the documentation, communication, or monitoring of the processes or controls, not the evaluation or alignment of the performance metrics. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Key Performance Indicators, page 183.

NEW QUESTION: 429
Warning banners on login screens for laptops provided by an organization to its employees are an example of which type of control?
A. Corrective
B. Preventive
C. Detective
D. Deterrent
Answer: (SHOW ANSWER)
Warning banners on login screens serve as deterrent controls. Deterrent controls are designed to discourage individuals from attempting unauthorized actions by warning them of potential consequences.
* Purpose of Warning Banners
* Warning banners provide clear notice to users, both authorized and unauthorized, that their activities may be monitored and that unauthorized access is prohibited.
* They serve as a legal disclaimer, which can be crucial in prosecuting unauthorized access attempts.
* Effectiveness as a Deterrent Control
* The primary function of a warning banner is to deter potential intruders by making them aware of the surveillance and legal implications of unauthorized access.
* For authorized users, it reinforces awareness of the organization's security policies and acceptable use agreements.
* Comparison with Other Control Types
* A. Corrective: These controls are used to correct or restore systems after an incident.
* B. Preventive: These controls are designed to prevent security incidents from occurring.
* C. Detective: These controls are used to detect and alert about security incidents.
* D. Deterrent: These controls are intended to discourage individuals from performing unauthorized activities.
References

* Sybex-CISSP-Official-Study-Guide-9-Edition.pdf, p. 829, detailing the role of warning banners as deterrent controls.

NEW QUESTION: 430

An organization has adopted an emerging technology without following proper processes. Which of the following is the risk practitioner's BEST course of action to address this risk?

freedam.net

A. Accept the risk because the technology has already been adopted.
B. Propose a transfer of risk to a third party with subsequent monitoring.
C. Conduct a risk assessment to determine risk exposure.
D. Recommend to senior management to decommission the technology.
Answer: (SHOW ANSWER)
Conducting a risk assessment allows the organization to evaluate the exposure created by adopting the technology. This step ensures informed decision-making and aligns with the principles of Risk Identification and Assessment for managing emerging risks effectively.

NEW QUESTION: 431
A Software as a Service (SaaS) provider has determined that the risk of a client's sensitive data being compromised is low. Which of the following is the client's BEST course of action?
A. Implement additional controls to address the risk
B. Accept the risk based on the provider's risk assessment
C. Review the provider's independent audit results
D. Ensure the contract includes breach notification requirements
Answer: (SHOW ANSWER)
Instead of relying solely on the provider's internal assessment, the client should validate control effectiveness throughindependent audit reports(e.g., SOC 2 Type II). These provide third-party assurance.
Reference:CRISC Manual - Domain 3, Slide 304-305

NEW QUESTION: 432
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?
A. Risk management
B. Change management
C. Problem management
D. Quality management
Answer: (SHOW ANSWER)
The key to controlling escalating costs when an organization is having new software implemented under contract is change management, which is the process of identifying, evaluating, approving, and implementing changes to the project scope, schedule, budget, or quality1. Change management can help to control escalating costs by:
* Establishing a clear and agreed-upon baseline for the project deliverables, requirements, and expectations, and ensuring that they are aligned with the contract terms and conditions2.

* Defining and enforcing a formal and consistent change control process, which includes the roles and responsibilities, the criteria and methods, and the documentation and communication of the changes3.
* Assessing and prioritizing the proposed changes, and determining their impact and feasibility, and their alignment with the project objectives and constraints4.
* Obtaining the approval and authorization of the relevant stakeholders, such as the project sponsor, the project manager, the contractor, or the customer, before implementing the changes5.
* Monitoring and measuring the performance and outcome of the changes, and ensuring that they are delivered within the agreed scope, schedule, budget, and quality6.
References =
* Change Management - CIO Wiki
* Project Scope Management - CIO Wiki
* Change Control - CIO Wiki
* Change Impact Analysis - CIO Wiki
* Change Approval - CIO Wiki
* Change Evaluation - CIO Wiki

NEW QUESTION: 433
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?
A. Percentage of high-risk vulnerabilities missed
B. Number of high-risk vulnerabilities outstanding
C. Defined thresholds for high-risk vulnerabilities
D. Percentage of high-risk vulnerabilities addressed
Answer: (SHOW ANSWER)
A key control indicator (KCI) is a metric that measures the effectiveness of a control in mitigating a risk. A good KCI for a vulnerability management program should reflect how well the program is reducing the exposure to high-risk vulnerabilities. The percentage of high-risk vulnerabilities addressed is a KCI that shows the proportion of identified high-risk vulnerabilities that have been remediated or mitigated within a defined time frame. This KCI can help monitor the progress and performance of the vulnerability management program and identify areas for improvement.
The other options are not the best KCI for a vulnerability management program because they do not measure the effectiveness of the control. The percentage of high-risk vulnerabilities missed is a measure of the completeness of the vulnerability scanning process, not the control. The number of high-risk vulnerabilities outstanding is a measure of the current risk exposure, not the control. The defined thresholds for high-risk vulnerabilities are a measure of the risk appetite, not the control. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3: IT Risk Assessment, Section 3.4: Risk Indicators, p. 133-134.

NEW QUESTION: 434
An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

A. Risk mitigation
B. Risk avoidance
C. Risk acceptance
D. Risk transfer
Answer: (SHOW ANSWER)
The risk treatment response that should be reflected in the risk register when an IT department decides to keep the data center in-house instead of outsourcing it to an overseas location is risk avoidance. Risk avoidance is a risk response strategy that involves eliminating the source of the risk, or changing the plan or scope of the activity, to avoid the risk altogether. Risk avoidance can help to reduce the risk exposure and impact to zero, by removing the possibility of the risk occurrence. In this case, the IT department avoids the risk of outsourcing the data center to an overseas location, which could involve various threats, vulnerabilities, and uncertainties, such as data security, legal compliance, service quality, communication, or cultural issues. By keeping the data center in-house, the IT department maintains the control and ownership of the data center, and eliminates the potential risk associated with the outsourcing. Risk mitigation, risk acceptance, and risk transfer are not the correct risk treatment responses, as they do not reflect the actual decision and action taken by the IT department, and they do not eliminate the risk source or occurrence. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 51.

NEW QUESTION: 435
Who should be accountable for monitoring the control environment to ensure controls are effective?
A. Risk owner
B. Security monitoring operations
C. Impacted data owner
D. System owner
Answer: (SHOW ANSWER)
The risk owner is the person or entity that has the accountability and authority to manage a risk. The risk owner should be accountable for monitoring the control environment to ensure controls are effective, as they are responsible for implementing, maintaining, and improving the risk controls, and for reporting and communicating the risk status and performance. The risk owner should also ensure that the controls are aligned with the risk appetite and tolerance of the enterprise, and that they support the achievement of the enterprise's objectives and value creation. References = Most Asked CRISC Exam Questions and Answers. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 244.

NEW QUESTION: 436
Which of the following will MOST likely change as a result of the decrease in risk appetite due to a new privacy regulation?
A. Key risk indicator (KRI) thresholds
B. Risk trends
C. Key performance indicators (KPIs)
D. Risk objectives
Answer: (SHOW ANSWER)

KRI thresholds are the levels or points that trigger an action or a response when a KRI reaches or exceeds them. They reflect the risk appetite of the organization, which is the amount and type of risk that it is willing to accept in pursuit of its objectives. A new privacy regulation may reduce the risk appetite of the organization, as it may impose stricter requirements and penalties for non-compliance. Therefore, the organization may need to adjust its KRI thresholds to lower levels, to ensure that it can identify and manage privacy risks more effectively and proactively

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 437
Which of the following BEST prevents control gaps in the Zero Trust model when implementing in the environment?
A. Relying on multiple solutions for Zero Trust
B. Utilizing rapid development during implementation
C. Establishing a robust technical architecture
D. Starting with a large initial scope
Answer: C (LEAVE A REPLY)
Zero Trust Model:
Zero Trust security model assumes that threats can exist both inside and outside the network. Every access request must be authenticated, authorized, and encrypted.
Preventing Control Gaps:
A robust technical architecture ensures comprehensive and consistent security controls across the entire network.
It integrates various security measures, such as microsegmentation, strong authentication, continuous monitoring, and least privilege access, to create a unified defense strategy.
Other Options:
Relying on Multiple Solutions:Can lead to fragmentation and inconsistencies in security controls.
Utilizing Rapid Development:May introduce vulnerabilities if security is not properly integrated.
Starting with a Large Initial Scope:Can be overwhelming and difficult to manage effectively, leading to potential gaps.
References:
The CISSP Study Guide emphasizes the importance of a strong and cohesive technical architecture in implementing Zero Trust effectively (Sybex CISSP Study Guide, Chapter 8: Principles of Security Models, Design, and Capabilities) .

NEW QUESTION: 438
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:
A. reduce the likelihood of future events
B. restore availability
C. reduce the impact of future events
D. address the root cause
Answer: (SHOW ANSWER)
Implementing a file corruption detection tool as a risk response strategy will help to reduce the impact of future events, as it will enable the organization to identify and correct the corrupted files before they cause further damage or loss. A file corruption detection tool is a software that scans and verifies the integrity and validity of the files, and alerts the users or administrators of any anomalies or errors. This helps to minimize the disruption and downtime caused by the data corruption incidents, and to preserve the quality and reliability of the data. Implementing a file corruption detection tool will not reduce the likelihood of future events, as it does not prevent or mitigate the causes or sources of the data corruption incidents. It will not restore availability, as it does not recover or restore the corrupted files, but only detects them. It will not address the root cause, as it does not analyze or eliminate the underlying factors that lead to the data corruption incidents. References = CRISC Certified in Risk and Information Systems Control - Question215; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 215.

NEW QUESTION: 439
A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:
A. mitigation plans for threat events should be prepared in the current planning period.
B. this risk scenario is equivalent to more frequent but lower impact risk scenarios.
C. the current level of risk is within tolerance.
D. an increase in threat events could cause a loss sooner than anticipated.
Answer: (SHOW ANSWER)
The risk practitioner should explain to senior management that mitigation plans for threat events should be prepared in the current planning period, as this would demonstrate a proactive and responsible approach to risk management. Mitigation plans are documents that outline the actions and resources needed to reduce the likelihood and/or impact of a specific risk scenario. Mitigation plans should include the following elements:
Risk scenario description and risk ID
Risk owner and other stakeholders
Risk response strategy and objectives
Risk response actions and tasks
Resources, costs, and benefits
Roles and responsibilities
Timeline and milestones

Performance indicators and monitoring mechanisms
Contingency plans and triggers
Mitigation plans help to address the gap between the current and desired risk levels and align the risk response with the organizational risk appetite and objectives. Mitigation plans also facilitate the communication, coordination, and collaboration among the risk owners and other stakeholders involved in the risk response process. Mitigation plans should be prepared in the current planning period, as this would allow the organization to act timely and effectively in the event of a low frequency threat event. Preparing mitigation plans in advance would also help to avoid or minimize the potential harm to the organization and its reputation.
The other options are not the best ways to communicate the associated risk to senior management. Explaining that this risk scenario is equivalent to more frequent but lower impact risk scenarios may not accurately reflect the true nature and severity of the risk. Explaining that the current level of risk is within tolerance may not convey the urgency and importance of addressing the risk. Explaining that an increase in threat events could cause a loss sooner than anticipated may not provide a clear and actionable solution for the risk. References = Four steps for managing risk at the CEO level, IT Risk Resources | ISACA, How to Communicate Risk to Stakeholders | Anitian

NEW QUESTION: 440
Which of the following would MOST likely require a risk practitioner to update the risk register?
A. An alert being reported by the security operations center.
B. Development of a project schedule for implementing a risk response
C. Completion of a project for implementing a new control
D. Engagement of a third party to conduct a vulnerability scan
Answer: (SHOW ANSWER)
The completion of a project for implementing a new control would most likely require a risk practitioner to update the risk register. The risk register is a document that records the identified risks, their analysis, and their responses. The completion of a project for implementing a new control means that a risk response has been executed and a new control has been established. This may affect the likelihood and/or impact of the related risks, and the residual risk level. Therefore, the risk practitioner should update the risk register to reflect the current status and outcome of the risk response and the new control. The other options are not as likely to require a risk practitioner to update the risk register, as they are related to the reporting, planning, or assessment of the risks or the controls, not the implementation or completion of the risk response or the new control. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.4: IT Risk Response, page 87.

NEW QUESTION: 441
Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?
A. Likelihood rating
B. Control effectiveness
C. Assessment approach

D. Impact rating

Answer: (SHOW ANSWER)

The risk register element that is most likely to be updated if the attack surface or exposure of an asset is reduced is the likelihood rating, as this reflects the probability or frequency of a risk event occurring. The attack surface or exposure of an asset is the measure of the extent and accessibility of the asset to potential threats or attackers. If the attack surface or exposure of an asset is reduced, the likelihood of the asset being compromised or damaged by a risk event is also reduced. Therefore, the likelihood rating of the risk should be updated accordingly. The other options are not the risk register elements that are most likely to be updated if the attack surface or exposure of an asset is reduced, although they may be affected or influenced by it.

Control effectiveness is the measure of how well the risk controls reduce the risk level or achieve the control objectives. Assessment approach is the method or technique used to identify, analyze, and evaluate the risks.

Impact rating is the measure of the magnitude or severity of the consequences of a risk event on the asset or the organization. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 54.

NEW QUESTION: 442

Which of the following is the MOST important reason to communicate risk assessments to senior management?

A. To ensure actions can be taken to align assessment results to risk appetite

B. To ensure key risk indicator (KRI) thresholds can be adjusted for tolerance

C. To ensure awareness of risk and controls is shared with key decision makers

D. To ensure the maturity of the assessment program can be validated

Answer: (SHOW ANSWER)

Communicating risk assessments to senior management is crucial for ensuring that key decision-makers are aware of the organization's risk landscape. This awareness enables informed decision-making regarding risk responses, resource allocation, and strategic planning. It also fosters a risk-aware culture throughout the organization.

Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 3: Risk Response and Reporting, Section: Risk Communication.

NEW QUESTION: 443

Which of the following events is MOST likely to trigger the need to conduct a risk assessment?

A. An incident resulting in data loss

B. Changes in executive management

C. Updates to the information security policy

D. Introduction of a new product line

Answer: (SHOW ANSWER)

Conducting a risk assessment is a critical process that helps organizations identify, evaluate, and prioritize risks that could impact their objectives. The introduction of a new product line is most likely to trigger the need for a risk assessment due to the following reasons:
Introduction of a New Product Line (Answer D):
Significance: Launching a new product involves significant changes to business processes, technologies, and possibly market dynamics. It introduces new elements that could affect the organization's risk profile.
Complexity and Uncertainty: New products often come with unknown risks and uncertainties. Understanding these risks is crucial to ensure they are managed effectively.
Impact on Operations: A new product can impact various facets of the organization, including production, supply chain, IT infrastructure, and customer support. Assessing risks helps in planning and mitigating potential disruptions.
Compliance and Regulatory Considerations: New products might have to comply with new regulations or standards, necessitating a review of associated risks.
Comparison with Other Options:
A: An incident resulting in data loss:
Purpose: While incidents like data loss are serious and require immediate response and investigation, they typically trigger incident management and post-incident reviews rather than a full risk assessment.
B: Changes in executive management:
Purpose: Changes in leadership can influence the strategic direction and priorities of the organization, but they do not inherently introduce new operational risks that necessitate an immediate risk assessment.
C: Updates to the information security policy:
Purpose: Policy updates are often based on previously identified risks and aim to mitigate them. They are more about adjusting controls rather than reassessing the risk landscape completely.
References:
ISACA CRISC Review Manual, Chapter 2, "IT Risk Assessment," which highlights the importance of conducting risk assessments in response to significant organizational changes, such as the introduction of new products, which can significantly alter the risk profile of the organization. This aligns with the need to reassess risks to ensure appropriate controls and mitigation strategies are in place for new initiatives.

NEW QUESTION: 444
A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:
A. management.
B. tolerance.
C. culture.
D. analysis.
Answer: C (LEAVE A REPLY)
Risk culture is the system of values and behaviors present in an organization that shapes risk decisions of management and employees1. Risk culture influences how the organization perceives, responds to, and manages the risks that may affect its objectives, operations, or assets2.

The scenario described in the question best demonstrates an organization's risk culture, because it shows how the management team's attitude and actions towards risk are driven by the organization's values and goals. In this case, the organization's risk culture is characterized by:
A high risk appetite and tolerance, which means that the organization is willing to take and accept significant risks in order to achieve its strategic objectives of launching a new product and penetrating new markets A low risk awareness and sensitivity, which means that the organization does not pay enough attention or consideration to the potential IT risk factors, threats, and vulnerabilities that may affect its product development and market entry A weak risk governance and control, which means that the organization does not have adequate or effective policies, procedures, or mechanisms to identify, assess, respond, or monitor the IT risks and their impacts References = Risk Culture of Companies | ERM - Enterprise Risk Management Initiative ..., Taking control of organizational risk culture | McKinsey

NEW QUESTION: 445
Following a review of a third-party vendor, it is MOST important for an organization to ensure:
A. results of the review are accurately reported to management.
B. identified findings are reviewed by the organization.
C. results of the review are validated by internal audit.
D. identified findings are approved by the vendor.
Answer: (SHOW ANSWER)
A review of a third-party vendor is a process that involves examining and evaluating the performance, quality, and compliance of the vendor that provides a product or service to the organization1. A review of a third-party vendor can help to identify and address the risks and issues that may arise from the vendorrelationship, such as data breaches, service disruptions, contract violations, or reputation damage2.
Following a review of a third-party vendor, it is most important for an organization to ensure that the results of the review are accurately reported to management, as this will enable the management to make informed and timely decisions and actions based on the findings and recommendations of the review. Accurate reporting of the results of the review will also help to establish and maintain the trust and transparency between the organization and the vendor, and to demonstrate the accountability and responsibility of the organization for its vendor risk management3. Identified findings are reviewed by the organization, results of the review are validated by internal audit, and identified findings are approved by the vendor are not the most important things to ensure following a review of a third-party vendor, as they do not provide the same level of impact and value as accurate reporting of the results of the review. Identified findings are reviewed by the organization is a process that involves analyzing and interpreting the outcomes and implications of the review of a third-party vendor, and determining the appropriate risk responses and actions to address the findings4.
This is an important step in the vendor risk management process, but it is not the most important thing to ensure following a review of a third-party vendor, as it does not communicate or inform the management or the vendor of the results of the review. Results of the review are validated by internal audit is a process that involves verifying and confirming the accuracy and reliability of the review of a third-party vendor, and providing assurance and advice on the adequacy and effectiveness of the vendor risk management. This is an important step in the vendor risk management process, but it is not the most important thing to ensure

following a review of a third-party vendor, as it does not report or share the results of the review with the management or the vendor. Identified findings are approved by the vendor is a process that involves obtaining the consent and agreement of the vendor on the outcomes and recommendations of the review of a third-party vendor, and ensuring their cooperation and compliance with the risk responses and actions. This is an important step in the vendor risk management process, but it is not the most important thing to ensure following a review of a third-party vendor, as it does not report or inform the management of the results of the review. References = 1: The guide to third-party vendor reviews - TerraTrue HQ | TerraTrue2: 4 Tips For Organizations To Evaluate Third-Party Vendors - Forbes Advisor3: Vendor Risk Management: Best Practices for 2023 - Venminder4: [Risk and Information Systems Control Study Manual, Chapter 3: Risk Response, Section 3.1: Risk Response Options, pp. 113-115.] : [IT Risk Resources | ISACA] : Who Is Considered a Third Party or Vendor? - Venminder : [Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.1: Risk Identification, pp. 57-59.] : [Risk and Information SystemsControl Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.] :
[Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.1: Control Design, pp. 233-235.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.2: Control Implementation, pp. 243-245.] : [Risk and Information Systems Control Study Manual, Chapter 5: Information Systems Control Design and Implementation, Section 5.3: Control Monitoring and Maintenance, pp. 251-253.]

NEW QUESTION: 446
Which of the following would BEST help to ensure that suspicious network activity is identified?
A. Analyzing intrusion detection system (IDS) logs
B. Analyzing server logs
C. Using a third-party monitoring provider
D. Coordinating events with appropriate agencies
Answer: (SHOW ANSWER)
An intrusion detection system (IDS) is a network security tool that monitors and analyzes network traffic for signs of malicious or suspicious activity, such as unauthorized access, data exfiltration, malware infection, or denial-of-service attack. An IDS can detect and alert the organization to potential threats based on predefined rules or signatures, or based on anomalies or deviations from normal network behavior. An IDS can also generate logs that record the details of the network events and incidents, such as the source, destination, content, and context of the network traffic. By analyzing the IDS logs, the organization can identify and validate the suspicious network activity, and determine its scope, impact, and root cause. The organization can also use the IDS logs to support the incident response and remediation process, and to improve the network security and resilience. The other options are less effective ways to ensure that suspicious network activity is identified. Analyzing server logs can provide some information about the network activity, but it may not be sufficient or timely to detect and validate the suspicious or malicious activity, as server logs only capture the events or activities that occur on the server, and not on the entire network. Using a third-party monitoring provider can help to outsource the network monitoring and analysis

function, but it may not be the best option, as it may introduce additional risks, such as data privacy, vendor reliability, or service quality issues. Coordinating events with appropriate agencies can help to share information and resources with other organizations or authorities, such as law enforcement, regulators, or industry peers, but it may not be the best option, as it may depend on the availability and cooperation of the agencies, and it may not be feasible or desirable to disclose the network activity to external parties. References = Monitoring for Suspicious Network Activity: Key Tips to Secure Your Network 1

NEW QUESTION: 447
Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:
A. communicate risk trends to stakeholders.
B. assign ownership of emerging risk scenarios.
C. highlight noncompliance with the risk policy
D. identify threats to emerging technologies.
Answer: (SHOW ANSWER)
The primary purpose of using key risk indicators (KRIs) to illustrate changes in the risk profile is to communicate risk trends to stakeholders. KRIs are metrics that provide an early warning of increasing risk exposure in various areas of the organization. By using KRIs to illustrate changes in the risk profile, the organization can communicate the risk trends to the stakeholders, such as the board, senior management, business units, and external parties, and enable them to take appropriate actions to manage the risk. Assigning ownership of emerging risk scenarios, highlighting noncompliance with the risk policy, and identifying threats to emerging technologies are other possible purposes, but they are not as important as communicating risk trends to stakeholders. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 12; CRISC Review Manual, 6th Edition, page 215.

NEW QUESTION: 448
The MAIN reason for creating and maintaining a risk register is to:
A. assess effectiveness of different projects.
B. define the risk assessment methodology.
C. ensure assets have low residual risk.
D. account for identified key risk factors.
Answer: (SHOW ANSWER)
A risk register is a tool used to identify, assess, and prioritize risks in an organization. It typically includes a detailed description of each identified risk, an assessment of its likelihood and potential impact, and a plan for managing or mitigating the risk1. A risk register is usually created at the beginning of a project or a process, and is updated regularly throughout the risk management life cycle2.
The main reason for creating and maintaining a risk register is to account for identified key risk factors. This means that the risk register helps to:
Document and track all the relevant risks that may affect the project or the organization, and their sources, causes, and consequences Provide a comprehensive and consistent view of the risk profile and exposure of the project or the organization Support the decision-making and prioritization of the risk responses and

controls, based on the risk appetite and tolerance of the project or the organization Communicate and report the risk information and status to the stakeholders and regulators, and ensure transparency and accountability Enable the continuous improvement and learning from the risk management process and outcomes3 References = What is a risk register and why is it important?, Purpose of a risk register: Here's what a risk register is used for, Risk Register: A Project Manager's Guide with Examples [2024], Risk Register - Wikipedia

NEW QUESTION: 449
An organization is developing a risk universe to create a holistic view of its overall risk profile. Which of the following is the GREATEST barrier to achieving the initiative's objectives?
A. Lack of cross-functional risk assessment workshops within the organization
B. Lack of common understanding of the organization's risk culture
C. Lack of quantitative methods to aggregate the total risk exposure
D. Lack of an integrated risk management system to aggregate risk scenarios
Answer: (SHOW ANSWER)
Lack of common understanding of the organization's risk culture is the greatest barrier to achieving the initiative's objectives, because it hinders the alignment and integration of risk management across the organization. Risk culture is the set of shared values, beliefs, and behaviors that influence how risk is perceived and managed in an organization. A risk universe is a comprehensive and structured representation of all the sources and types of risk that an organization faces. Developing a risk universe requires a common understanding of the organization's risk culture, as it affects the risk appetite, tolerance, and strategy of the organization. Lack of cross-functional risk assessment workshops, lack of quantitative methods to aggregate the total risk exposure, and lack of an integrated risk management system are all challenges that may affect thedevelopment of a risk universe, but they are not the greatest barrier, as they can be overcome with appropriate tools and techniques. References = Risk and Information Systems Control Study Manual, Chapter
2, Section 2.2.1, page 44

NEW QUESTION: 450
Which of the following is MOST important to consider when determining the value of an asset during the risk identification process?
Freecram.net
A. The criticality of the asset
B. The monetary value of the asset
C. The vulnerability profile of the asset
D. The size of the asset's user base
Answer: (SHOW ANSWER)
The criticality of the asset is the most important factor to consider when determining the value of an asset during the risk identification process, because it reflects the importance or significance of the asset to the organization's objectives or functions, and the potential impact or consequence of losing or compromising the asset. An asset is a resource or capability that has value to the organization, such as data, systems, applications, infrastructure, or people. The value of an asset is a measure of the worth or benefit of the asset

to the organization, and the cost or loss of the asset to the organization. The risk identification process is a process of systematically identifying the sources and types of risk that an organization faces, and estimating their likelihood and impact. The criticality of the asset is the most important factor, as it helps to prioritize and focus on the assets that have the highest value and impact, and to determine the appropriate level of protection and investment for the assets. The monetary value of the asset, the vulnerability profile of the asset, and the size of the asset's user base are all possible factors to consider when determining the value of an asset, but they are not the most important factor, as they do not directly reflect the criticality of the asset to the organization's objectives or functions. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.1, page 83

NEW QUESTION: 451
Which of the following situations would cause the GREATEST concern around the integrity of application logs?
A. Weak privileged access management controls
B. Lack of a security information and event management (SIEM) system
C. Lack of data classification policies
D. Use of hashing algorithms
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 452
Which of the following is the MOST important key performance indicator (KPI) to establish in the service level agreement (SLA) for an outsourced data center?
A. Percentage of systems included in recovery processes
B. Number of key systems hosted
C. Average response time to resolve system incidents
D. Percentage of system availability
Answer: D (LEAVE A REPLY)
The percentage of system availability is the most important key performance indicator (KPI) to establish in the service level agreement (SLA) for an outsourced data center. This KPI measures the uptime or reliability of the systems hosted by the data center provider, and reflects the ability of the provider to meet the customer' s expectations and requirements for system performance and accessibility. A high percentage of system availability indicates that the provider is delivering consistent and quality service, while a low percentage of system availability indicates that the provider is experiencing frequent or prolonged system

failures or disruptions, which can negatively affect the customer's business operations and reputation. Therefore, the percentage of system availability is a critical factor for evaluating the effectiveness and efficiency of the data center provider, and should be clearly defined and monitored in the SLA. The other options are not the most important KPIs to establish in the SLA for an outsourced data center, as they do not directly measure the quality or reliability of the service provided. The percentage of systems included in recovery processes is a measure of the scope or coverage of the disaster recovery plan (DRP) of the data center provider, but it does not indicate how well the provider can execute the DRP or restore the systems in the event of a disaster. The number of key systems hosted is a measure of the capacity or utilization of the data center provider, but it does not indicate how efficiently or securely the provider can manage the systems. The average response time to resolve system incidents is a measure of the responsiveness or agility of the data center provider, but it does not indicate how effectively or proactively the provider can prevent or mitigate system incidents. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3, Section
3.2.3.4, Page 140.

NEW QUESTION: 453
From a risk management perspective, which of the following is the PRIMARY purpose of conducting a root cause analysis following an incident?
A. To reduce incident response times defined in SLAs
B. To satisfy senior management expectations for incident response
C. To ensure risk has been reduced to acceptable levels
D. To minimize the likelihood of future occurrences
Answer: (SHOW ANSWER)
Root cause analysis helps identify the fundamental reason for an incident, allowing the enterprise to implement controls that reduce the probability of recurrence.
Reference:CRISC Manual - Domain 4, Slide 248

NEW QUESTION: 454
What is the PRIMARY role of the application owner when changes are being introduced into an existing environment?
A. Determining possible losses due to downtime during the changes
B. Updating control procedures and documentation
C. Approving the proposed changes based on impact analysis
D. Notifying owners of affected systems after the changes are implemented
Answer: (SHOW ANSWER)
The application owner must formally approve changes after reviewing impact-per ISACA's change management and governance frameworks that assign control over operational fallouts to functional owners .

NEW QUESTION: 455
Which of the following is the ULTIMATE objective of utilizing key control indicators (KCIs) in the risk management process?

A. To provide a basis for determining the criticality of risk mitigation controls
B. To provide early warning signs of a potential change in risk level
C. To provide benchmarks for assessing control design effectiveness against industry peers
D. To provide insight into the effectiveness of the intemnal control environment
Answer: (SHOW ANSWER)
Key control indicators (KCIs) are metrics that measure the performance of a control in reducing the causes, consequences, or likelihood of a risk. They help to evaluate the adequacy and efficiency of the internal control environment, which is the set of policies, procedures, and practices that support the achievement of organizational objectives and the management of risks. By monitoring KCIs, organizations can identify and address any gaps or weaknesses in their internal controls and ensure that they are operating as intended.
References
*ISACA CRISC Review Manual, 7th Edition, Domain 3: Risk Response, Section 3.2.2: Control Design and Implementation
*KRI Framework for Operational Risk Management | Workiva
*What is the difference between key risk indicators and key control indicators?

NEW QUESTION: 456
Which of the following is the MOST important criteria for selecting key risk indicators (KRIs)?
A. Historical data availability
B. Implementation and reporting effort
C. Ability to display trends
D. Sensitivity and reliability
Answer: (SHOW ANSWER)
Sensitivity and reliability are the most important criteria for selecting KRIs, as they indicate how well the KRIs reflect the changes in the risk level and how consistent and accurate the KRIs are in measuring the risk. Sensitivity means that the KRIs should respond quickly and proportionally to the variations in the risk exposure, and provide early warning signals of potential risk events. Reliability means that the KRIs should be based on valid and verifiable data sources, and produce consistent and comparable results over time and across different units or functions. Historical data availability, implementation and reporting effort, and ability to display trends are also useful criteria, but they are not as critical as sensitivity and reliability.
References:
*ISACA, Risk IT Framework, 2nd Edition, 2019, p. 751
*ISACA, Risk and Information Systems Control Review Manual, 7th Edition, 2020, p. 2122

NEW QUESTION: 457
An organization allows programmers to change production systems in emergency situations. Which of the following is the BEST control?
A. Implementing an emergency change authorization process
B. Periodically reviewing operator logs
C. Limiting the number of super users
D. Reviewing the programmers' emergency change reports

Answer: (SHOW ANSWER)
Implementing an emergency change authorization process is the best control for an organization that allows programmers to change production systems in emergency situations, because it helps to ensure that the changes are justified, approved, documented, and tested before they are implemented, and that they are monitored and reviewed after they are implemented. An emergency change is a change that is required to resolve or prevent a critical issue or incident that may affect the availability, performance, or security of the production systems. A production system is a system that is used to support or enable the operational or business functions or processes of the organization. An emergency change authorization process is a process that defines the roles and responsibilities, criteria and procedures, and tools and techniques for managing and controlling the emergency changes. Implementing an emergency change authorization process is the best control, as it helps to minimize the risks and impacts of the emergency changes, and to maintain the integrity and reliability of the production systems. Periodically reviewing operator logs, limiting the number of super users, and reviewing the programmers' emergency change reports are all possible controls for an organization that allows programmers to change production systems in emergency situations, but they are not the best control, as they do not provide a comprehensive and consistent approach to the emergency change management. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.4.1, page 208

NEW QUESTION: 458
Which of the following BEST reduces the likelihood of employees unintentionally disclosing sensitive information to outside parties?
A. Sensitive information classification and handling policies
B. Anti-malware controls on endpoint devices
C. Regular employee security awareness training
D. An egress intrusion detection system (IDS)
Answer: (SHOW ANSWER)

NEW QUESTION: 459
Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?
A. Recovery time objective (RTO)
B. Cost-benefit analysis
C. Business impact analysis (BIA)
D. Cyber insurance coverage
Answer: (SHOW ANSWER)
Business impact analysis (BIA) is the most helpful tool in identifying loss magnitude during risk analysis of a new system, as it involves estimating the potential financial and operational losses resulting from the disruption or degradation of the system. Recovery time objective (RTO), cost-benefit analysis, and cyber insurance coverage are not the most helpful tools, as they are more related to the recovery, evaluation, and transfer of the risk, respectively, rather than the identification of the loss magnitude. References = CRISC Review Manual, 7th Edition, page 108.

NEW QUESTION: 460

An organization has decided to implement a new Internet of Things (IoT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

Freecram.net

A. Develop new IoT risk scenarios.

B. Implement IoT device monitoring software.

C. Introduce controls to the new threat environment.

D. Engage external security reviews.

Answer: (SHOW ANSWER)

The first thing that should be done when addressing security concerns associated with a new Internet of Things (IoT) solution is to develop new IoT risk scenarios. IoT is a network of physical devices, such as sensors, cameras, appliances, etc., that are connected to the internet and can collect, process, and exchange data. IoT introduces new security concerns, such as privacy, confidentiality, integrity, availability, and accountability of the data and devices, as well as new threats and vulnerabilities, such as unauthorized access, manipulation, or disruption of the data and devices. Developing new IoT risk scenarios is the first thing that should be done, because it helps to identify, analyze, and evaluate the potential risks that could affect the IoT solution's objectives or operations. Developing new IoT risk scenarios also helps to select the most appropriate and effective controls to minimize the risks, such as avoiding, reducing, transferring, or accepting the risks. The other options are not the first thing that should be done, although they may be part of or derived from the IoT risk scenarios. Implementing IoT device monitoring software, introducing controls to the new threat environment, and engaging external security reviews are all activities that can help to support or improve the security of the IoT solution, but they do not necessarily identify, analyze, or evaluate the risks that could affect the IoT solution. References = 1

NEW QUESTION: 461

Which of the following would be MOST useful to senior management when determining an appropriate risk response?

A. A comparison of current risk levels with established tolerance

B. A comparison of cost variance with defined response strategies

C. A comparison of current risk levels with estimated inherent risk levels

D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: (SHOW ANSWER)

A comparison of current risk levels with established tolerance is the most useful information for senior management when determining an appropriate risk response, as it shows the gap between the actual risk exposure and the desired risk exposure of the enterprise. This gap indicates the need and urgency for risk response actions, and helps senior management to prioritize and allocate resources for risk mitigation. A comparison of current risk levels with established tolerance also reflects the effectiveness of the existing risk management process and controls, and enables senior management to monitor and adjust the risk strategy and objectives accordingly. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 234. CRISC by Isaca Actual Free Exam Q&As, Question 9. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 234. CRISC Sample Questions 2024, Question 234.

NEW QUESTION: 462
An organization has experienced several incidents of extended network outages that have exceeded tolerance.
Which of the following should be the risk practitioner's FIRST step to address this situation?
A. Recommend additional controls to address the risk.
B. Update the risk tolerance level to acceptable thresholds.
C. Update the incident-related risk trend in the risk register.
D. Recommend a root cause analysis of the incidents.
Answer: (SHOW ANSWER)
The first step for the risk practitioner to address the situation of extended network outages that have exceeded tolerance is to recommend a root cause analysis of the incidents. A root cause analysis is a process of identifying and resolving the underlying causes of a problem or an event. By performing a root cause analysis, the risk practitioner can determine why the network outages occurred, what factors contributed to them, and how they can be prevented or reduced in the future. Recommending additional controls, updating the risk tolerance level, and updating the incident-related risk trend are possible steps that may follow the root cause analysis, but they are not the first step. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 4; CRISC Review Manual, 6th Edition, page 153.

NEW QUESTION: 463
Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?
A. Organizational structure and job descriptions
B. Risk appetite and risk tolerance
C. Industry best practices for risk management
D. Prior year's risk assessment results
Answer: (SHOW ANSWER)
The best way to enable a risk practitioner to understand management's approach to organizational risk is to know the risk appetite and risk tolerance of the organization. Risk appetite is the amount and type of risk that an organization is willing to pursue, retain, or take in order to achieve its objectives. Risk tolerance is the amount and type of risk that an organization is willing to accept in relation to specific performance measures, such as availability, reliability, or security. Risk appetite and risk tolerance reflect the management's attitude, preferences, and expectations towards risk, and guide the risk management process, such as risk identification, assessment, response, and monitoring. The other options are not as effective as knowing the risk appetite and risk tolerance, although they may provide some input or context for understanding the management's approach to organizational risk. References = Risk and Information Systems Control Study Manual, Chapter
1, Section 1.2.1, page 1-8.

NEW QUESTION: 464

The GREATEST concern when maintaining a risk register is that:
A. impacts are recorded in qualitative terms.
B. executive management does not perform periodic reviews.
C. IT risk is not linked with IT assets.
D. significant changes in risk factors are excluded.
Answer: (SHOW ANSWER)
A risk register is a tool that records and tracks the identified risks, their causes, impacts, likelihood, responses, and owners. The greatest concern when maintaining a risk register is that significant changes in risk factors are excluded. Risk factors are the internal and external variables that influence the occurrence and impact of risks. Risk factors can change over time due to changes in the business environment, the IT landscape, the threat landscape, or the regulatory requirements. If the risk register does not reflect the significant changes in risk factors, it may not provide an accurate and current view of the enterprise's risk profile and may not support effective risk management decisions and actions. The other options are not as concerning as the exclusion of significant changes in risk factors, as they involve different aspects of the risk register:
Impacts are recorded in qualitative terms means that the risk register uses descriptive scales, such as low, medium, and high, to measure the potential consequences of the risks. This may not be asprecise or consistent as quantitative measures, such as monetary values or percentages, but it does not necessarily affect the validity or usefulness of the risk register.
Executive management does not perform periodic reviews means that the risk register is not regularly evaluated and updated by the senior leaders of the enterprise. This may indicate a lack of management commitment or oversight for risk management, but it does not directly affect the quality or completeness of the risk register.
IT risk is not linked with IT assets means that the risk register does not associate the identified risks with the specific IT resources, such as hardware, software, data, or services, that are affected by or contribute to the risks. This may limit the visibility and traceability of the risks, but it does not necessarily affect the identification or assessment of the risks. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.2.2.2, pp. 21-22.

NEW QUESTION: 465
Which of the following is the PRIMARY objective of the three lines model for risk management?
A. The model shows how to effectively apply oversight and monitoring for the purpose of mitigating risk.
B. The model states that only employees are responsible for IT risk management.
C. The model provides clear delineation of roles and responsibilities for managing IT risk.
D. The model stipulates that senior management is responsible for IT risk management activities.
Answer: (SHOW ANSWER)
The Three Lines Model (formerly "three lines of defense") is a governance concept used in CRISC and other ISACA frameworks. Its primary objective is to clarify who does what in risk management:
* First line - operational management: owns and manages risk, operates controls.
* Second line - risk management/compliance: provides expertise, support, and monitoring for risk and controls.

* Third line - internal audit: provides independent assurance on the effectiveness of governance, risk management, and control.
CRISC-related notes on the three lines state that:
* The most significant benefit of using the three lines model is that it clarifies essential roles of key stakeholders.
* Risk owner is a risk management role that is part of the first line of defense.
* Establishing a risk management framework is a direct responsibility of the second line.
* Operational management is the function that manages risk according to the three lines model.
So the core of the model is role and responsibility clarity, which directly supports effective governance and accountability for risk.
Why the other options are incorrect:
* A. Oversight and monitoring are important outcomes, but they are consequences of properly defined roles rather than the model's primary objective.
* B. "Only employees are responsible" is false; accountability spans board, senior management, management, staff, and independent assurance.
* **D. Senior management does have key responsibilities, but the model explicitly distributes risk roles across multiple lines, not just senior management.
Therefore, the PRIMARY objective is correctly captured by C: providing clear delineation of roles and responsibilities for managing IT risk.

NEW QUESTION: 466
Which of the following is a security concern regarding data transmission in a corporate environment?
A. Internal email communications are not encrypted.
B. Data transmission within the corporate network is not encrypted.
C. Internally created documents are not automatically classified.
D. Data transmission across public networks is not encrypted.
Answer: D (LEAVE A REPLY)
Data transmission across public networks is the greatest risk because public networks are inherently insecure and vulnerable to interception. Encryption is critical to protecting data confidentiality during transmission over such networks. Lack of encryption internally is less risky due to controlled environments. Classification helps but does not protect data in transit. Email encryption is important but less critical compared to public network transmission risks.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 467
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:
A. a threat.
B. a vulnerability.
C. an impact
D. a control.
Answer: B (LEAVE A REPLY)
A vulnerability is a weakness or flaw that can be exploited by a threat to cause harm or damage to an asset. Employees holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges, is a behavior that best represents a vulnerability, as it bypasses the security control of the ID badge system, and allows unauthorized or unauthenticated access to the premises. This behavior can increase the risk of physical or logical security breaches, such as theft, vandalism, sabotage, or espionage. References = CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 258. Most Asked CRISC Exam Questions and Answers, Question 10. ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 258. CRISC by Isaca Actual Free Exam Q&As, Question 9.

NEW QUESTION: 468
Which of the following is the BEST metric to measure the effectiveness of an organization's disaster recovery program?
A. Percentage of applications subject to disaster recovery tests
B. Number of personnel dedicated to the disaster recovery program
C. Number of disaster recovery tests performed per year
D. Percentage of systems meeting defined recovery objectives
Answer: (SHOW ANSWER)
Meeting defined RTOs and RPOs indicates that the DR plan can achieve its intended goals under real conditions. This metric directly reflects the effectiveness and reliability of the program.
Reference:CRISC Manual - Domain 4, Slide 452, 554

NEW QUESTION: 469
To help identify high-risk situations, an organization should:
A. continuously monitor the environment.
B. develop key performance indicators (KPIs).
C. maintain a risk matrix.
D. maintain a risk register.
Answer: (SHOW ANSWER)
To help identify high-risk situations, an organization should continuously monitor the environment, as it can help to detect and respond to any changes or emerging risks that may affect the organization's objectives and strategy. Continuous monitoring can also provide timely and relevant feedback and information to the decision-makers and stakeholders, and enable them to adjust the risk strategy and response actions

accordingly. Continuous monitoring can also help to ensure that the risk management process is aligned with the organization's risk appetite and tolerance, and supports the achievement of the organization's goals and value creation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 243. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 243. CRISC Sample Questions 2024, Question 243.

NEW QUESTION: 470

Which of the following is the MOST useful indicator to measure the efficiency of an identity and access management process?

Freecram.net

A. Number of tickets for provisioning new accounts

B. Average time to provision user accounts

C. Password reset volume per month

D. Average account lockout time

Answer: (SHOW ANSWER)

The average time to provision user accounts is the most useful indicator to measure the efficiency of an identity and access management (IAM) process, because it reflects how quickly and smoothly the process can grant access to the appropriate users. The average time to provision user accounts can be calculated by dividing the total time spent on provisioning user accounts by the number of user accounts provisioned in a given period. A lower average time indicates a more efficient IAM process, as it means that users can access the resources they need without unnecessary delays or errors. A higher average time may indicate problems or bottlenecks in the IAM process, such as manual steps, complex workflows, lack of automation, or insufficient resources. The average time to provision user accounts can also be compared across different applications, systems, or business units to identify areas for improvement or best practices. The other options are less useful indicators to measure the efficiency of an IAM process. The number of tickets for provisioning new accounts shows the demand for the IAM process, but not how well the process meets the demand. The password reset volume per month shows the frequency of password-related issues, but not how effectively the IAM process handles them. The average account lockout time shows the impact of account lockouts on user productivity, but not how efficiently the IAM process prevents or resolves them. References = Top Identity and Access Management Metrics

NEW QUESTION: 471

A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

A. Risk manager

B. Control owner

C. Control tester

D. Risk owner

Answer: (SHOW ANSWER)

The control owner is the person who is responsible for ensuring that the control is designed to effectively address risk. The control owner is also responsible for implementing, operating, monitoring, and maintaining

the control. The control owner should ensure that the control is aligned with the risk owner's risk appetite and tolerance, and that the control is periodically reviewed and updated to reflect changes in the risk environment.
The risk manager, the control tester, and the risk owner are not directly responsible for the design of the control, although they may provide input, feedback, or approval. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.2, page 1-15.

NEW QUESTION: 472
It was discovered that a service provider's administrator was accessing sensitive information without the approval of the customer in an Infrastructure as a Service (IaaS) model. Which of the following would BEST protect against a future recurrence?
A. Data encryption
B. Intrusion prevention system (IPS)
C. Two-factor authentication
D. Contractual requirements
Answer: (SHOW ANSWER)
The best option to protect against a future recurrence of unauthorized access by a service provider's administrator is D. Contractual requirements. Data encryption, intrusion prevention system, and two-factor authentication are all technical measures that can enhance the security of the data stored in the Infrastructure as a Service (IaaS) model, but they do not prevent the service provider's administrator from accessing the data if they have the necessary credentials, keys, or permissions. Contractual requirements, on the other hand, are legal obligations that bind the service provider to respect the customer's privacy and confidentiality, and to limit the access to the data to only authorized and necessary personnel. Contractual requirements can also specify the penalties or remedies for any breach of contract, which can deter the service provider's administrator from violating the terms of the agreement. Therefore, contractual requirements are the most effective way to protect against a future recurrence of unauthorized access by a service provider's administrator12
1: What is Data Encryption? | Forcepoint 2: The elements of a contract: understanding contract requirements - Juro

NEW QUESTION: 473
A bank is experiencing an increasing incidence of customer identity theft. Which of the following is the BEST way to mitigate this risk?
A. Implement monitoring techniques.
B. Implement layered security.
C. Outsource to a local processor.
D. Conduct an awareness campaign.
Answer: (SHOW ANSWER)
The best way to mitigate the risk of customer identity theft is to implement layered security. Layered security is a defense-in-depth approach that applies multiple and diverse security controls at different levels and stages of the information system and the data lifecycle. Layered security can include physical, technical, and

administrative controls, such as locks, firewalls, encryption, authentication, authorization, backup, audit, and policy. Layered security can help to protect the customer data and identity from unauthorized access, use, modification, disclosure, or destruction, by creating multiple barriers and deterrents for potential attackers, and by reducing the impact and likelihood of a successful breach. Layered security can also help to comply with the legal and regulatory requirements and standards for data privacy and protection, such as the Gramm- Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and the Payment Card Industry Data Security Standard (PCI DSS)123. The other options are not the best way to mitigate the risk of customer identity theft, although they may be useful or complementary to layered security. Implementing monitoring techniques is a part of the layered security approach, but it is not sufficient, as it mainly focuses on detecting and responding to the incidents, rather than preventing or deterring them. Outsourcing to a local processor is a business decision that may or may not improve the security of the customer data and identity, depending on the quality and reliability of the service provider, and the terms and conditions of the outsourcing contract.
Conducting an awareness campaign is a good practice that can help to educate and inform the customers and the employees about the common types, methods, and indicators of identity theft, and the best practices and precautions to prevent or report it, but it does not directly apply or enforce any security controls to the information system or the data.

NEW QUESTION: 474
The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:
A. vulnerability scans.
B. recurring vulnerabilities.
C. vulnerabilities remediated,
D. new vulnerabilities identified.
Answer: (SHOW ANSWER)
According to the Key Performance Indicators for Vulnerability Management article, the number of vulnerabilities remediated is a key performance indicator that measures the effectiveness of a vulnerability remediation program. This KPI indicates how many vulnerabilities have been successfully mitigated or fixed within a given time frame. A higher number can imply that the organization is effectively managing its exposures and reducing its risk level. The number of vulnerabilities remediated can also be compared with the number of new vulnerabilities identified to evaluate the progress and performance of the vulnerability remediation program. References = Key Performance Indicators for Vulnerability Management

NEW QUESTION: 475
The risk associated with a high-risk vulnerability in an application is owned by the:
A. security department.
B. business unit
C. vendor.
D. IT department.
Answer: (SHOW ANSWER)

A high-risk vulnerability in an application is a system flaw or weakness in the application's code that can be exploited by a malicious actor, potentially leading to a security breach. The risk associated with a high-risk vulnerability in an application is the possibility and impact of such a breach occurring. The risk owner of a high-risk vulnerability in an application is the person or entity who has the authority and responsibility for managing the risk. The risk owner should be able to define the risk appetite, assess the risk level, select and implement the risk response, monitor and report the risk status, and ensure the risk alignment with the business objectives and strategy. The risk owner of a high-risk vulnerability in an application is the business unit, which is the organizational unit that operates the application and derives value from it. The businessunit understands the business needs and expectations of the application, and the potential consequences of a security breach. The business unit also has the resources and incentives to address the risk effectively and efficiently. Therefore, the business unit is the most appropriate risk owner of a high-risk vulnerability in an application. References = Why Assigning a Risk Owner is Important and How to Do It Right, CRISC 351-400 topic3, Foundations of Project Management : Week 2.

NEW QUESTION: 476
An updated report from a trusted research organization shows that attacks have increased in the organization's industry segment. What should be done FIRST to integrate this data into risk assessments?
A. Average the ransomware attack frequencies together
B. Revise the threat frequency for ransomware attack types
C. Adjust impact amounts based on the average ransom
D. Use the new frequency as the maximum value in a Monte Carlo simulation
Answer: (SHOW ANSWER)
New threat intelligence primarily impacts the frequency component of risk calculations.
CRISC states:
"When new information about threats is available, it must be incorporated into risk assessment by adjusting threat event frequencies in related scenarios."
* A and D are statistical manipulations, not practical first steps.
* C addresses impact, not likelihood.
Hence, B. Revise the threat frequency is correct.
CRISC Reference: Domain 2 - IT Risk Assessment, Topic: Incorporating Threat Intelligence.

NEW QUESTION: 477
Which of the following BEST helps to identify significant events that could impact an organization?
Vulnerability analysis
A. Heat map analysis
B. Control analysis
C. Scenario analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 478
Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

A. Creating a data classification scheme
B. Identifying events impacting continuity of operations
C. Analyzing previous risk assessment results
D. Identifying critical information assets
Answer: D (LEAVE A REPLY)
The first step in conducting a BIA is to identify critical information assets. This involves determining which assets are essential to the organization's operations and would have the most significant impact if disrupted. Understanding these assets sets the foundation for assessing potential impacts and developing appropriate recovery strategies.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 2: IT Risk Assessment, Section: Business Impact Analysis.

NEW QUESTION: 479
The PRIMARY reason for prioritizing risk scenarios is to:
A. provide an enterprise-wide view of risk
B. support risk response tracking
C. assign risk ownership
D. facilitate risk response decisions.
Answer: (SHOW ANSWER)
The primary reason for prioritizing risk scenarios is to facilitate risk response decisions. Risk scenarios are hypothetical situations that describe the possible causes, events, and consequences of a risk. Prioritizing risk scenarios is the process of ranking the risk scenarios according to their level of importance, urgency, or impact. Prioritizing risk scenarios helps to facilitate risk response decisions, which are the choices made to address the risks, such as avoiding, transferring, mitigating, or accepting the risks. Prioritizing risk scenarios helps to allocate the resources and efforts to the most significant or critical risk scenarios, and to select the most appropriate and effective risk responses. Prioritizing risk scenarios also helps to communicate and justify the risk response decisions to the stakeholders, and to monitor and report the risk status and performance. Providing an enterprise-wide view of risk, supporting risk response tracking, and assigning risk ownership are not the primary reasons for prioritizing risk scenarios, as they are either the inputs or the outputs of the risk prioritization process, and they do not address the primary need of responding to the risks.
References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 50.

NEW QUESTION: 480
A vendor's planned maintenance schedule will cause a critical application to temporarily lose failover capabilities. Of the following, who should approve this proposed schedule?
Pdfcram.net
A. Business continuity manager
B. Chief risk officer (CRO)
C. IT infrastructure manager
D. Business application owner
Answer: (SHOW ANSWER)

The business application owner is responsible for the application's performance and availability. Therefore, they should approve any maintenance schedules that could impact the application's functionality, including temporary loss of failover capabilities. Their approval ensures that the business implications are considered and that appropriate contingency plans are in place.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: IT Operations and Maintenance.

NEW QUESTION: 481
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?
A. Include the new risk scenario in the current risk assessment.
B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment
Answer: A (LEAVE A REPLY)
A new risk scenario without controls means that there is a potential threat or event that could adversely affect the organization's objectives, and there are no existing measures to prevent or reduce the impact or likelihood of the risk. Therefore, the most appropriate action is to include the new risk scenario in the current risk assessment, so that the risk practitioner can analyze the risk, evaluate its severity and priority, and recommend suitable controls to mitigate the risk. By including the new risk scenario in the current risk assessment, the risk practitioner can ensure that the risk register is updated and reflects the current risk profile of the organization.
The other options are not appropriate because they either ignore the new risk scenario, delay the risk assessment process, or remove valuable information from the risk register. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.1, page 95.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 482
Which of the following should be the PRIMARY driver for the prioritization of risk responses?
A. Residual risk
B. Risk appetite
C. Mitigation cost
D. Inherent risk
Answer: B (LEAVE A REPLY)

* Risk Appetite:
* Risk appetite defines the level of risk that an organization is willing to accept in pursuit of its objectives. It serves as a benchmark for evaluating and prioritizing risk responses.
* Prioritizing Risk Responses:
* When determining how to address risks, the primary consideration should be whether the residual risk falls within the organization's risk appetite.
* If a risk exceeds the appetite, it needs to be mitigated, transferred, or avoided. If it is within the appetite, it might be accepted.
* Influence of Other Factors:
* Residual Risk: Important but must be evaluated against the risk appetite to determine if it is acceptable.
* Mitigation Cost: Relevant for decision-making but secondary to aligning with risk appetite.
* Inherent Risk: Initial risk assessment before controls are applied, but prioritization is based on residual risk and risk appetite.
* References:
* The CRISC Review Manual highlights the role of risk appetite in guiding the prioritization of risk responses (CRISC Review Manual, Chapter 3: Risk Response and Mitigation, Section 3.2.1 Prioritizing Risk Responses).

NEW QUESTION: 483
Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization's risk register?
A. Risk taxonomy
B. Risk response
C. Risk appetite
D. Risk ranking
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, risk taxonomy is the system of classification and categorization of risks based on common characteristics and attributes. Risk taxonomy is necessary to enable an IT risk register to be consolidated with the rest of the organization's risk register, because it helps to ensure consistency, comparability, and alignment of the risks across the organization. Risk taxonomy also helps to facilitate the communication, reporting, and aggregation of the risks. The other options are not the correct answers, because they are not essential for consolidating the risk registers. Risk response is the action taken to address the risk, which may vary depending on the risk level and strategy. Risk appetite is the amount and type of risk that an organization is willing to accept, which may differ across the organization's units and functions. Risk ranking is the process of prioritizing the risks based on their impact and likelihood, which may change over time and context. References = CRISC Review Manual, 7th Edition, Chapter 2, Section 2.1.2, page 69.

NEW QUESTION: 484
Which of the following should be the PRIMARY objective of promoting a risk-aware culture within an organization?

A. Better understanding of the risk appetite
B. Improving audit results
C. Enabling risk-based decision making
D. Increasing process control efficiencies
Answer: (SHOW ANSWER)
The primary objective of promoting a risk-aware culture within an organization is enabling risk-based decision making, because this helps the organization to achieve its goals and objectives while managing its risks effectively and efficiently. A risk-aware culture is one where everyone understands the organization's approach to risk, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example. A risk-aware culture also fosters communication, collaboration, and learning about risk across the organization. By promoting a risk-aware culture, the organization can empower its employees to make informed and balanced decisions that consider both the potential benefits and the potential risks of their actions. This can enhance the organization's performance, resilience, and competitiveness in a dynamic and uncertain environment. References = Risk IT Framework, ISACA, 2022, p. 17

NEW QUESTION: 485
Risk aggregation in a complex organization will be MOST successful when:
A. using the same scales in assessing risk
B. utilizing industry benchmarks
C. using reliable qualitative data for risk Hems
D. including primarily low-level risk factors
Answer: (SHOW ANSWER)
Risk aggregation in a complex organization will be MOST successful when using the same scales in assessing risk, because it can help to ensure the consistency and comparability of the risk assessment results across different units, levels, and domains of the organization. Using the same scales in assessing risk can also help to avoid the potential errors or biases that may arise from using different scales, such as overestimating or underestimating the risk exposure, or misaligning the risk appetite and tolerance. The other options are not as important as using the same scales in assessing risk, because:
* Option B: Utilizing industry benchmarks is a good way to improve the quality and validity of the risk assessment results, but it does not ensure the success of the risk aggregation, which is the process of combining and consolidating the risk assessment results into a holistic and comprehensive view of the risk profile and exposure of the organization.
* Option C: Using reliable qualitative data for risk items is a useful way to capture and describe the risk items, which are the sources and causes of the risks, but it does not ensure the success of the risk aggregation, which is the process of quantifying and measuring the risk items, and their likelihood and impact on the business objectives and processes.
* Option D: Including primarily low-level risk factors is a necessary way to identify and assess the risk factors, which are the characteristics and attributes of the risks, but it does not ensure the success of the risk aggregation, which is the process of prioritizing and ranking the risk factors, and their significance and relevance to the organization's strategy and goals. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 105.

NEW QUESTION: 486
Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?
A. Vulnerability and threat analysis
B. Control remediation planning
C. User acceptance testing (UAT)
D. Control self-assessment (CSA)
Answer: (SHOW ANSWER)
Information systems control deficiencies are the weaknesses or flaws in the design or implementation of the controls that are intended to ensure the confidentiality, integrity, availability, and reliability of the information systems and resources. Information systems control deficiencies may reduce the effectiveness or efficiency of the controls, and expose the organization to various risks, such as unauthorized access, data loss, system failure, etc.
Reviewing results from control self-assessment (CSA) is the best way to identify information systems control deficiencies, because CSA is a process of evaluating and verifying the adequacy and effectiveness of the information systems controls, using the input and feedback from the individuals or groups that are involved or responsible for the information systems activities or functions. CSA can help the organization to identify and document the information systems control deficiencies, and to align them with the organization's information systems objectives and requirements.
CSA can be performed using various techniques, such as questionnaires, surveys, interviews, workshops, etc.
CSA can also be integrated with the organization's governance, risk management, and compliance functions, and aligned with the organization's policies and standards.
The other options are not the best ways to identify information systems control deficiencies, because they do not provide the same level of detail and insight that CSA provides, and they may not be relevant or actionable for the organization.
Vulnerability and threat analysis is a process of identifying and evaluating the weaknesses or flaws in the organization's assets, processes, or systems that can be exploited or compromised by the potential threats or sources of harm that may affect the organization's objectives or operations. Vulnerability and threat analysis can help the organization to assess and prioritize the risks, and to design and implement appropriate controls or countermeasures to mitigate or prevent the risks, but it is not the best way to identify information systems control deficiencies, because it does not indicate whether the existing information systems controls are adequate and effective, and whether they comply with the organization's policies and standards.
Control remediation planning is a process of selecting and implementing the actions or plans to address or correct the information systems control deficiencies that have been identified, analyzed, and evaluated. Control remediation planning involves choosing one ofthe following types of control responses: mitigate, transfer, avoid, or accept. Control remediation planning can help the organization to improve and optimize the information systems controls, and to reduce or eliminate the information systems control deficiencies, but

it is not the best way to identify information systems control deficiencies, because it is a subsequent or follow-up process that depends on the prior identification of the information systems control deficiencies. User acceptance testing (UAT) is a process of verifying and validating the functionality and usability of the information systems and resources, using the input and feedback from the end users or customers that interact with the information systems and resources. UAT can help the organization to ensure that the information systems and resources meet the user or customer expectations and requirements, and to identify and resolve any issues or defects that may affect the user or customer satisfaction, but it is not the best way to identify information systems control deficiencies, because it does not focus on the information systems controls, and it may not cover all the relevant or significant information systems control deficiencies that may exist or arise. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 40-41, 47-48, 54-55, 58-59, 62-63 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 186 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 487
Which of the following key risk indicators (KRIs) provides the BEST insight into the risk associated with IT systems being unable to meet the required availability service level in the future?
A. Percentage of IT systems having defined incident management service levels
B. Percentage of IT systems having met the availability service level
C. Percentage of IT outsourced systems having met the availability service level
D. Percentage of IT systems routinely running at peak utilization
Answer: D (LEAVE A REPLY)
The percentage of IT systems routinely running at peak utilization serves as a leading indicator of potential future availability issues. Systems operating at or near full capacity are more susceptible to performance degradation or outages, which can impede their ability to meet service level agreements (SLAs). Monitoring this KRI allows organizations to proactively address capacity constraints before they impact system availability.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Key Risk Indicators.

NEW QUESTION: 488
Which of the following is MOST important for an organization to continuously manage after implementing a Zero Trust security model?
A. Privileged user access reviews
B. Integration with existing security protocols
C. Policy enforcement inconsistencies
D. Network segmentation errors
Answer: (SHOW ANSWER)
In a Zero Trust model, access is never implicitly trusted and must be continuously verified - making privileged access review critical.
ISACA CRISC guidance:

"Under the Zero Trust model, continuous validation and review of privileged user access is essential to prevent privilege escalation and insider threats." Integration and segmentation are design concerns; privileged access management is the ongoing control requirement.
Thus, A is correct.
CRISC Reference: Domain 4 - Risk and Control Monitoring and Reporting, Topic: Zero Trust and Continuous Authorization.

NEW QUESTION: 489
Which of the following is the PRIMARY purpose for ensuring senior management understands the organization's risk universe in relation to the IT risk management program?
A. To define effective enterprise IT risk appetite and tolerance levels
B. To execute the IT risk management strategy in support of business objectives
C. To establish business-aligned IT risk management organizational structures
D. To assess the capabilities and maturity of the organization's IT risk management efforts
Answer: (SHOW ANSWER)
Ensuring senior management understands the organization's risk universe in relation to the IT risk management program is primarily to define effective enterprise IT risk appetite and tolerance levels. This understanding is essential for setting the boundaries within which the organization is willing to operate regarding IT risks.
Defining Effective IT Risk Appetite and Tolerance Levels (Answer A):
Purpose: Senior management needs to understand the range and nature of IT risks to set appropriate risk appetite and tolerance levels.
Impact: This enables the organization to make informed decisions about which risks to accept, mitigate, transfer, or avoid.
Alignment: It ensures that the IT risk management strategy is aligned with the overall business objectives and risk posture of the organization.
Comparison with Other Options:
B: To execute the IT risk management strategy in support of business objectives:
Purpose: While important, it follows the definition of risk appetite and tolerance.
Limitation: Without understanding the risk universe, execution may be misaligned.
C: To establish business-aligned IT risk management organizational structures:
Purpose: Structural alignment is crucial but secondary to setting risk appetite and tolerance.
D: To assess the capabilities and maturity of the organization's IT risk management efforts:
Purpose: This is part of the ongoing process but not the primary purpose of understanding the risk universe.
References:
ISACA CRISC Review Manual, Chapter 1, "Governance", which discusses the importance of risk appetite and tolerance in the context of IT risk management.

NEW QUESTION: 490

An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

Freecram.net

A. Number of malicious activities occurring during staff members leave

B. Percentage of staff members seeking exception to the policy

C. Percentage of staff members taking leave according to the policy

D. Financial loss incurred due to malicious activities during staff members' leave

Answer: (SHOW ANSWER)

The best key performance indicator (KPI) of the effectiveness of the policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities is the percentage of staff members taking leave according to the policy. A KPI is a quantifiable measure that evaluates the performance of a process, activity, or outcome against a predefined target or objective. The percentage of staff members taking leave according to the policy is the best KPI, because it directly measures the compliance and adherence of the staff members to the policy, which is the main objective of the policy. The policy aims to reduce the risk of malicious insider activities by forcing the staff members to take a break from their work, which can help to deter, detect, or prevent any fraudulent or unauthorized actions, such as data theft, sabotage, or manipulation12. The percentage of staff members taking leave according to the policy can also help to evaluate the effectiveness and efficiency of the policy implementation and enforcement, and to identify and address any gaps or issues in the policy design or execution. The other options are not the best KPI, although they may be related or influential to the policy effectiveness. The number of malicious activities occurring during staff members' leave is a measure of the occurrence and impact of the risk events that the policy aims to mitigate, but it is not a direct measure of the policy performance or compliance. The number of malicious activities occurring during staff members' leave may also be affected by other factors or controls, such as the security systems, the audit procedures, or the external threats, which may not reflect the policy effectiveness. The percentage of staff members seeking exception to the policy is a measure of the resistance or dissatisfaction of the staff members to the policy, but it is not a direct measure of the policy performance or compliance. The percentage of staff members seeking exception to the policy may also be influenced by other factors or circumstances, such as the workload, the personal preferences, or the organizational culture, which may not indicate the policy effectiveness. The financial loss incurred due to malicious activities during staff members' leave is a measure of the consequence and severity of the risk events that the policy aims to mitigate, but it is not a direct measure of the policy performance or compliance. The financial loss incurred due to malicious activities during staff members' leave may also vary depending on the type, scale, or frequency of the malicious activities, or the recovery or compensation actions, which may not represent the policy effectiveness. References = How To Measure Risk Management KPI & Metrics - ERM Software, Key Performance Indicators (KPIs): The Ultimate Guide - ClearPoint Strategy

NEW QUESTION: 491

Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

A. The organization's structure has not been updated

B. Unnecessary access permissions have not been removed.

C. Company equipment has not been retained by IT
D. Job knowledge was not transferred to employees m the former department
Answer: B (LEAVE A REPLY)
The greatest concern for an IT risk practitioner when an employee transfers to another department is that unnecessary access permissions have not been removed. Unnecessary access permissions are the access rights or privileges that are no longer needed, relevant, or appropriate for the employee's new role or responsibility.
If these access permissions are not removed, they may pose a significant security risk, as the employee may be able to access, modify, or delete sensitive or critical data and systems that are not related to their current function. This may result in data leakage, fraud, sabotage, or compliance violations. The other options are not as concerning as unnecessary access permissions, as they are related to the organizational, operational, or knowledge aspects of the employee transfer, not the security or risk aspects of the employee transfer.
References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 492
Which of the following BEST facilitates the identification of emerging risk?
A. Performing scenario-based assessments
B. Reviewing audit reports annually
C. Conducting root cause analyses
D. Engaging a risk-focused audit team
Answer: (SHOW ANSWER)
Performing scenario-based assessments is a proactive approach that allows organizations to anticipate potential future events and assess their impact. This method helps in identifying emerging risks by exploring hypothetical situations and their possible outcomes. It enables organizations to prepare for unforeseen events by understanding how different scenarios could affect their operations and objectives.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 2: IT Risk Assessment, Section: Risk Identification Techniques.

NEW QUESTION: 493
Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?
A. Disruption to business processes
B. Cost of implementation
C. Implementation of unproven applications
D. Increase in attack surface area
Answer: (SHOW ANSWER)

NEW QUESTION: 494
An organization has outsourced its ERP application to an external SaaS provider. Which of the following provides the MOST useful information to identify risk scenarios involving data loss?
A. Data classification schemes

B. Industry data breach reports
C. Data storage locations
D. Data flow documentation
Answer: (SHOW ANSWER)
Data flow documentation provides insight into how and where data moves, stored, or processed. It helps identify vulnerable points in the data lifecycle where data loss can occur.
Reference:CRISC Manual - Domain 1: Governance, Slide 240

NEW QUESTION: 495
An organization's Internet-facing server was successfully attacked because the server did not have the latest security patches. The risk associated with poor patch management had been documented in the risk register and accepted. Who should be accountable for any related losses to the organization?
A. Risk owner
B. IT risk manager
C. Server administrator
D. Risk practitioner
Answer: (SHOW ANSWER)
The risk owner is the person who should be accountable for any related losses to the organization, because they are the person who has the authority and responsibility to manage the risk and its associated controls. The risk owner is also the person who accepts the risk and its residual level, and who monitors and reports on the risk status and performance. The IT risk manager, the server administrator, and the risk practitioner are all involved in the risk management process, but they are not the person who should be accountable for the risk and its outcomes, as they do not have the ultimate decision-making power and accountability for the risk.
References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.1.1, page 79

NEW QUESTION: 496
Which of the following is MOST important to review when an organization needs to transition the majority of its employees to remote work during a crisis?
A. Customer notification plans
B. Capacity management
C. Access management
D. Impacts on IT project delivery
Answer: (SHOW ANSWER)
Capacity management is crucial when transitioning employees to remote work during a crisis. It involves ensuring that the IT infrastructure can handle increased loads and that resources are available to support remote operations effectively.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 497
A PRIMARY objective of disaster recovery is to:
A. Improve infrastructure of physical locations
B. Restore critical business and IT services
C. Recover financial data and statements
D. Maintain operational processes and connectivity
Answer: (SHOW ANSWER)
Disaster Recovery (DR) focuses on restoring IT and business services to support essential operations after a disruption.
ISACA defines:
"The primary objective of disaster recovery is the timely restoration of critical IT systems and services necessary to support business operations." Recovery of financial records or facilities are secondary components.
Therefore, B. Restore critical business and IT services is correct.
CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Business Continuity and Disaster Recovery Planning.

NEW QUESTION: 498
A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?
A. Add a digital certificate
B. Apply multi-factor authentication
C. Add a hash to the message
D. Add a secret key
Answer: (SHOW ANSWER)
A digital certificate is a document that contains the public key and the identity of the owner of the public key, and is signed by a trusted third party called a certificate authority (CA)1. A digital certificate can be used to ensure the message reaches the intended recipient without alteration, by using the following steps2:
The sender encrypts the message with the recipient's public key, which can only be decrypted by the recipient' s private key. This ensures the confidentiality of the message, as only the intended recipient can read it.
The sender signs the message with their own private key, which can be verified by anyone who has their public key. This ensures the integrity and authenticity of the message, as it proves that the message has not been tampered with and that it comes from the sender.

The sender attaches their digital certificate to the message, which contains their public key and their identity, and is signed by a CA. This ensures the validity and trustworthiness of the sender's public key and identity, as it confirms that they have been verified by a CA.
The recipient receives the message and the digital certificate, and verifies the signature of the CA on the digital certificate. This ensures that the digital certificate is genuine and has not been forged or revoked.
The recipient uses the public key from the digital certificate to verify the signature of the sender on the message. This ensures that the message has not been altered and that it comes from the sender.
The recipient uses their own private key to decrypt the message. This ensures that they can read the message.
Therefore, adding a digital certificate is the best way to ensure the message reaches the intended recipient without alteration, as it provides encryption, digital signature, and certificate verification, which are the three main components of secure email communication3. Applying multi-factor authentication, adding a hash to the message, and adding a secret key are not the best ways to ensure the message reaches the intended recipient without alteration, as they do not provide all the components of secure email communication.
Applying multi- factor authentication is a technique that requires the user to provide two or more pieces of evidence to prove their identity, such as a password, a code, or a biometric factor4. Multi-factor authentication can enhance the security of the email account, but it does not protect the message itselffrom being intercepted, modified, or impersonated. Adding a hash to the message is a technique that involves applying a mathematical function to the message to generate a fixed-length value, called a hash or a digest, that uniquely represents the message5.
A hash can be used to verify the integrity of the message, as any change in the message will result in a different hash. However, ahash does not provide confidentiality or authenticity of the message, as it does not encrypt themessage or identify the sender. Adding a secret key is a technique that involves using a single key, known only to the sender and the recipient, to encrypt and decrypt the message6. A secret key can provide confidentiality of the message, as only the sender and the recipient can read it. However, a secret key does not provide integrity or authenticity of the message, as it does not prevent the message from being altered or spoofed. Moreover, a secret key requires a secure way of exchanging the key between the sender and the recipient, which may not be feasible or reliable over email. References = 1: What is a digital certificate? | Norton2: How to Send Secure Emails in 2023 | A Guide to Secure Email - ProPrivacy3: Secure Email: A Complete Guide for 2023 - StartMail4: What is Multi-Factor Authentication (MFA)? | Duo Security5: What is a Hash Function? | Definition and FAQs6: [What is Symmetric Encryption? | Definition and FAQs]

NEW QUESTION: 499
An organization has been made aware of a newly discovered critical vulnerability in a regulatory reporting system. Which of the following is the risk practitioner's BEST course of action?
A. Perform an impact assessment.
B. Perform a penetration test.
C. Request an external audit.
D. Escalate the risk to senior management.
Answer: (SHOW ANSWER)

The risk practitioner's best course of action when an organization has been made aware of a newly discovered critical vulnerability in a regulatory reporting system is to perform an impact assessment, as it involves estimating the potential consequences or damage that the vulnerability may cause to the system and its related business processes, and prioritizing the risk response accordingly. The other options are not the best courses of action, as they may not address the urgency or severity of the vulnerability, or may require the prior knowledge of the impact or risk level, respectively. References = CRISC Review Manual, 7th Edition, page
100.

NEW QUESTION: 500

An organization recently implemented a cybersecurity awareness program that includes phishing simulation exercises for all employees. What type of control is being utilized?

Freecram.net

A. Deterrent
B. Preventive
C. Compensating
D. Detective
Answer: (SHOW ANSWER)
Phishing simulation exercises are designed to educate users and reduce the likelihood of them falling for real phishing attacks. This is considered apreventive control, as it aims to stop incidents before they occur by changing behavior.
Reference:CRISC Manual - Domain 3, Slide 275-276

NEW QUESTION: 501
Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?
A. Failed login attempts
B. Simulating a denial of service attack
C. Absence of IT audit findings
D. Penetration test
Answer: (SHOW ANSWER)
A penetration test is a simulated cyberattack on a web infrastructure to evaluate its security posture and identify any vulnerabilities or weaknesses that could be exploited by an attacker. A penetration test is the best indicator of how well a web infrastructure protects critical information from an attacker, as it mimics the real-world scenarios and techniques that an attacker would use, and measures the effectiveness of the existing security controls and countermeasures. A penetration test can also provide recommendations for improving the security of the web infrastructure and reducing the risk exposure. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 236. CRISC by Isaca Actual Free Exam Q&As, Question 9. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 236. Most Asked CRISC Exam Questions and Answers, Question 10.

NEW QUESTION: 502
Which organizational role should be accountable for ensuring information assets are appropriately classified?
A. Data protection officer
B. Chief information officer (CIO)
C. Information asset custodian
D. Information asset owner
Answer: D (LEAVE A REPLY)
The organizational role that should be accountable for ensuring information assets are appropriately classified is the information asset owner, as they have the authority and responsibility to define the classification, retention, and disposal requirements for the information assets they own, and to manage the risk and controls related to the information assets. The other options are not the correct roles, as they have different roles and responsibilities related to the protection, governance, or maintenance of the information assets, respectively, rather than the classification of the information assets. References = CRISC Review Manual, 7th Edition, page 154.

NEW QUESTION: 503
Which of the following BEST enables senior management lo compare the ratings of risk scenarios?
A. Key risk indicators (KRIs)
B. Key performance indicators (KPIs)
C. Control self-assessment (CSA)
D. Risk heat map
Answer: D (LEAVE A REPLY)
A risk heat map is the best tool to enable senior management to compare the ratings of risk scenarios, as it provides a visual representation of the risk level and priority of each risk scenario, based on the combination of the likelihood and impact ratings, and the risk tolerance and appetite of the organization. Key risk indicators (KRIs), key performance indicators (KPIs), and control self-assessment (CSA) are not the best tools, as they are more related to the measurement, monitoring, or testing of the risk scenarios, respectively, rather than the comparison of the risk scenarios. References = CRISC Review Manual, 7th Edition, page 110.

NEW QUESTION: 504
Which of the following is the MOST important consideration when multiple risk practitioners capture risk scenarios in a single risk register?
A. Aligning risk ownership and control ownership
B. Developing risk escalation and reporting procedures
C. Maintaining up-to-date risk treatment plans
D. Using a consistent method for risk assessment
Answer: (SHOW ANSWER)
A risk register is a document that records and tracks the information and status of the identified risks and their responses. It includes the risk description, category, source, cause, impact, probability, priority, response, owner, action plan, status, etc.

A risk scenario is a description or representation of a possible or hypothetical situation or event that may cause or result in a risk for the organization. A risk scenario usually consists of three elements: a threat or source of harm, a vulnerability or weakness, and an impact or consequence.
Multiple risk practitioners are the individuals or groups that are involved or responsible for the identification, analysis, evaluation, and communication of the risks and their responses. They may include the risk owners, risk managers, risk analysts, risk consultants, risk auditors, etc.
A single risk register is a risk register that is shared or used by multiple risk practitioners across the organization, and that contains the information and status of all the risks and their responses that are relevant or applicable to the organization.
The most important consideration when multiple risk practitioners capture risk scenarios in a single risk register is using a consistent method for risk assessment, which is the process of determining the significance and urgency of the risks that may affect the organization's objectives and operations. Risk assessment involves measuring and comparing the likelihood and impact of various risk scenarios, and prioritizing them based on their magnitude and importance.
Using a consistent method for risk assessment when multiple risk practitioners capture risk scenarios in a single risk register ensures that the risk scenarios are captured and recorded in a uniform and standardized way, and that they are comparable and compatible with each other. It alsohelps to avoid or reduce the inconsistencies, discrepancies, or conflicts that may arise from the different perspectives, assumptions, or judgments of the multiple risk practitioners, and to ensure the accuracy, reliability, and validity of the risk register.
The other options are not the most important considerations when multiple risk practitioners capture risk scenarios in a single risk register, because they do not address the main challenge or issue that may arise from the multiple risk practitioners capturing risk scenarios in a single risk register, which is the lack of consistency or standardization in the risk assessment method.
Aligning risk ownership and control ownership means ensuring that the individuals or groups that are accountable and responsible for the risks and their responses are clearly defined and assigned, and that they have the authority and resources to perform their roles and duties. Aligning risk ownership and control ownership is important when multiple risk practitioners capture risk scenarios in a single risk register, but it is not the most important consideration, because it does not ensure that the risk scenarios are captured and recorded in a uniform and standardized way, and that they are comparable and compatible with each other.
Developing risk escalation and reporting procedures means establishing and implementing the processes and guidelines for communicating and sharing the information and status of the risks and their responses among the relevant stakeholders, and for escalating or transferring the risks and their responses to the appropriate levels or parties when necessary or required. Developing risk escalation and reporting procedures is important when multiple risk practitioners capture riskscenarios in a single risk register, but it is not the most important consideration, because itdoes not ensure that the risk scenarios are captured and recorded in a uniform and standardized way, and that they are comparable and compatible with each other.
Maintaining up-to-date risk treatment plans means updating and revising the actions or plans that are selected and implemented to address or correct the risks and their responses, based on the changes or developments that may occur in the risk environment or performance. Maintaining up-to-date risk treatment plans is important when multiple risk practitioners capture risk scenarios in a single risk register, but it is not

the most important consideration, because it does not ensure that the risk scenarios are captured and recorded in a uniform and standardized way, and that they are comparable and compatible with each other.
References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-
59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 178 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 505
A risk practitioner is defining metrics for security threats that were not identified by antivirus software. Which type of metric is being developed?
A. Key control indicator (KCI)
B. Key risk indicator (KRI)
C. Operational level agreement (OLA)
D. Service level agreement (SLA)
Answer: (SHOW ANSWER)
A KRI is a measure used by an organization to measure the health of a particular risk. In this case, the risk practitioner is developing a metric to measure the risk associated with security threats that were not identified by antivirus software12.
References
1Standardized Scoring for Security and Risk Metrics - ISACA
2Key Performance Indicators for Security Governance, Part 1 - ISACA

NEW QUESTION: 506
Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?
A. Standard operating procedures
B. SWOT analysis
C. Industry benchmarking
D. Control gap analysis
Answer: (SHOW ANSWER)
New risk exposures due to changes in the business environment are the possibilities and impacts of new or emerging threats or opportunities that may affect the organization's objectives, performance, or value creation, as a result of changes in the internal or external factors that influence the organization's operations, such as technology, competition, regulation, or customer behavior12.
The most helpful tool in identifying new risk exposures due to changes in the business environment is a SWOT analysis, which is a technique that involves identifying and analyzing the strengths, weaknesses, opportunities, and threats (SWOT) that are relevant to the organization's situation, goals, and capabilities34.
A SWOT analysis is the most helpful tool because it helps the organization to scan and assess the business environment, and to identify and prioritize the new or emerging risk exposures that may arise from the changes in the environment34.

A SWOT analysis is also the most helpful tool because it helps the organization to align and adapt its strategy and actions to the changes in the environment, and to leverage its strengths and opportunities, and mitigate its weaknesses and threats34.
The other options are not the most helpful tools, but rather possible sources or inputs that may be used in a SWOT analysis. For example:
Standard operating procedures are documents that describe the routine tasks and processes that are performed by the organization, and the policies and standards that govern them56. However, these documents are not the most helpful tools because they may not reflect or capture the changes in the business environment, and they may need to be revised or updated to address the new or emerging risk exposures56.
Industry benchmarking is a technique that involves comparing and contrasting the performance and practices of the organization with those of the similar or leadingorganizations in the same or related industry, and identifying the gaps or opportunities for improvement78. However, this technique is not the most helpful tool because it may not provide a comprehensive or holistic view of the business environment, and it may not align with the organization's specific situation, goals, or capabilities78.
Control gap analysis is a technique that involves assessing and evaluating the adequacy and effectiveness of the controls that are designed and implemented to mitigate the risks, and identifying and addressing the areas or aspects that need to be improved or added . However, this technique is not the most helpful tool because it is reactive rather than proactive, and it may not identify or anticipate the new or emerging risk exposures that may result from the changes in the business environment . References =
1: Risk IT Framework, ISACA, 2009
2: IT Risk Management Framework, University of Toronto, 2017
3: SWOT Analysis - ISACA1
4: SWOT Analysis: What It Is and When to Use It2
5: Standard Operating Procedure - Wikipedia3
6: How to Write Effective Standard Operating Procedures (SOP)4
7: Benchmarking - Wikipedia5
8: Benchmarking: Definition, Types, Process, Advantages & Examples6
Control Gap Analysis - ISACA7
Control Gap Analysis: A Step-by-Step Guide8

NEW QUESTION: 507
Which of the following stakeholders define risk tolerance for an enterprise?
A. IT compliance and IT audit
B. Regulators and shareholders
C. The board and executive management
D. Enterprise risk management (ERM)
Answer: (SHOW ANSWER)
Role of the Board and Executive Management:
The board of directors and executive management are responsible for setting the overall strategic direction of the organization, including its risk tolerance.

They have the authority and oversight necessary to define the levels of risk that the organization is willing to accept in pursuit of its objectives.
Defining Risk Tolerance:
Risk tolerance refers to the acceptable level of variation in performance relative to the achievement of objectives. It is essentially the degree of risk the organization is willing to endure.
The board and executive management establish risk tolerance based on the organization's strategic goals, capacity to absorb losses, and regulatory requirements.
Importance of Senior Leadership:
Senior leadership's involvement ensures that risk tolerance is aligned with the organization's overall strategy and risk appetite.
It provides a top-down approach to risk management, ensuring consistency and alignment across the organization.
Comparing Other Stakeholders:
IT Compliance and IT Audit:These functions are responsible for monitoring and ensuring adherence to policies but do not set risk tolerance.
Regulators and Shareholders:They influence risk management practices through external pressures but do not define risk tolerance directly.
Enterprise Risk Management (ERM):ERM frameworks support the implementation of risk management but the actual definition of risk tolerance comes from the board and executive management.
References:
The CRISC Review Manual discusses how senior management, including the board, is responsible for defining risk tolerance and ensuring it aligns with the organization's risk appetite (CRISC Review Manual, Chapter 1: Governance, Section 1.10 Risk Appetite, Tolerance, and Capacity) .

NEW QUESTION: 508
An effective control environment is BEST indicated by controls that:
A. minimize senior management's risk tolerance.
B. manage risk within the organization's risk appetite.
C. reduce the thresholds of key risk indicators (KRIs).
D. are cost-effective to implement
Answer: (SHOW ANSWER)
According to the CRISC Review Manual (Digital Version), an effective control environment is best indicated by controls that manage risk within the organization's risk appetite, as this reflects the alignment of thecontrol objectives and activities with the organization's strategic goals and risk preferences. The risk appetite is the amount and type of risk that the organization is willing to accept in pursuit of its objectives. Managing risk within the organization's risk appetite helps to:
Balance the potential benefits and costs of risk-taking and risk response Optimize the use of the organization's resources and capabilities Enhance the value and performance of the organization Foster a risk-aware culture that supports the organization's vision and mission References = CRISC Review Manual (Digital Version), Chapter 2: IT Risk Assessment, Section 2.3: IT Risk Assessment Process, pp. 93-941

NEW QUESTION: 509
Which of the following is the FIRST consideration to reduce risk associated with the storage of personal data?
A. Implement privacy training
B. Normalize the personal data
C. Minimize the collection of data
D. Encrypt the personal data
Answer: (SHOW ANSWER)
CRISC and privacy frameworks such as ISO/IEC 27701 and GDPR emphasize data minimization as the first step in managing privacy risk:
"Personal data collection must be limited to what is necessary for the specified purpose." If data is never collected, there's no need for storage, encryption, or training around it - thus reducing exposure and risk at the source.
Other options, while useful, come after minimizing collection:
* A and D address residual risk.
* B (normalization) affects data structure, not privacy risk reduction.
Hence, C. Minimize the collection of data is correct.
CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Privacy Risk Controls.

NEW QUESTION: 510
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:
A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.
C. verify Internet firewall control settings.
D. identify vulnerabilities in the system.
Answer: (SHOW ANSWER)
The primary reason for periodic penetration testing of Internet-facing applications is to identify vulnerabilities in the system, because this will help to improve the security and resilience of the applications and the data they process. A penetration test is a simulated cyberattack that aims to exploit the weaknesses and gaps in the security of an application or a system. A penetration test can reveal the vulnerabilities that may not be detected by other methods, such as automated scanning or code review. A penetration test can also measure the impact and severity of the vulnerabilities, as well as the effectiveness of the existing controls and defenses. A penetration test can also provide recommendations and solutions to remediate the vulnerabilities and prevent future attacks. Internet-facing applications are programs and services that are accessible from the internet, such as web applications, APIs, cloud services, or VPN gateways. Internet-facing applications are exposed to a variety of cyber threats, such as denial-of-service attacks, SQL injection attacks, cross-site scripting attacks, or credential stuffing attacks. These threats can compromise the confidentiality, integrity, and availability of the applications and the data they handle. Therefore, periodic penetration testing of Internet- facing applications is essential to identify vulnerabilities in the system and to protect the applications and the data from cyberattacks. References = Web Application Penetration Testing:

A Practical Guide - BrightSecurity1, The Basics of Web Application Penetration Testing | Turing2, Periodic Penetration Testing:
What is the best pentesting frequency ...

NEW QUESTION: 511
To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?
A. business owner
B. IT department
C. Risk manager
D. Third-party provider
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, the business owner is the person who has the authority and accountability for the achievement of the business objectives and the management of the associated risks. The business owner is ultimately responsible for ensuring that the IT services and solutions support the business needs and goals, and for accepting or rejecting the residual risks after the implementation of risk responses. Therefore, the business owner should own the risk associated with calculation errors, as they are the ones who will be affected by the potential impact of the errors on the financial data and decisions. References = CRISC Review Manual1, page 194.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 512
Which of the following will provide the BEST measure of compliance with IT policies?
A. Evaluate past policy review reports.
B. Conduct regular independent reviews.
C. Perform penetration testing.
D. Test staff on their compliance responsibilities.
Answer: (SHOW ANSWER)
Conducting regular independent reviews will provide the best measure of compliance with IT policies, as this ensures that the policies are implemented and followed consistently and effectively across the organization. Independent reviews can also identify any gaps, weaknesses, or violations in the compliance process, and recommend corrective actions or improvements. Independent reviews can be performed by internal or external auditors, regulators, or consultants, depending on the scope and purpose of the review. Evaluating

past policy review reports, performing penetration testing, and testing staff on their compliance responsibilities are not the best measures of compliance with IT policies, although they may be useful or complementary methods.
Evaluating past policy review reports can provide some historical and comparative data, but it may not reflect the current or accurate situation of the compliance status. Performing penetration testing can assess the security and vulnerability of the IT systems and networks, but it does not measure the compliance with all the IT policies, such as those related to governance, operations, or quality. Testing staff on their compliance responsibilities can evaluate the awareness and knowledge of the staff, but it does not measure the actual behaviour or performance of the staff in complying with the IT policies. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk and Control Monitoring and Reporting, page 187.

NEW QUESTION: 513
Which of The following BEST represents the desired risk posture for an organization?
A. Inherent risk is lower than risk tolerance.
B. Operational risk is higher than risk tolerance.
C. Accepted risk is higher than risk tolerance.
D. Residual risk is lower than risk tolerance.
Answer: (SHOW ANSWER)
The best representation of the desired risk posture for an organization is when the residual risk is lower than the risk tolerance. Residual risk is the remaining risk after the implementation of risk responses or controls. Risk tolerance is the acceptable level of risk that the organization is willing to take or bear. The desired risk posture is when the organization has reduced the residual risk to a level that is equal to or lower than the risk tolerance, which means that the organization has achieved its risk objectives and is comfortable with the remaining risk exposure. The other options are not the best representation of the desired risk posture, as they indicate that the organization has not effectively managed its risk. Inherent risk is lower than risk tolerance means that the organization has not identified or assessed its risk properly, as inherent risk is the risk before any controls or responses are applied. Operational risk is higher than risk tolerance means that the organization has not implemented or monitored its risk responses or controls adequately, as operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems. Accepted risk is higher than risk tolerance means that the organization has not aligned its risk appetite and risk tolerance, as accepted risk is the risk that the organization chooses to retain or take without any further action. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.3.1, page 2-23.

NEW QUESTION: 514
Which of the following MUST be captured in a risk treatment plan?
A. Risk owner
B. Senior management
C. Risk register details
D. Risk financial impact
Answer: (SHOW ANSWER)

A risk treatment plan (sometimes called a risk response plan) describes how selected risk treatments will be implemented, by whom, and by when. For the plan to be actionable and enforceable, every significant risk and its treatment must have a clearly assigned risk owner.
CRISC guidance emphasizes that:
* Accountability for risk treatment lies with the risk owner.
* A risk treatment plan primarily provides treatment for identified risk that exceeds risk tolerance and should specify responsibility for implementing the chosen risk treatment.
* Ensuring accountability and ownership is critical for the effectiveness of the risk management program.
While items such as financial impact and risk register references are useful supporting information, the one element that must be present for each treated risk is the person or role responsible for making sure the treatment is implemented and monitored.
Therefore:
* A. Risk owner - REQUIRED in every risk treatment plan entry.
* B. "Senior management" is too generic; they may approve the plan but are not always the specific treatment owners.
* C. "Risk register details" are normally linked to or referenced, but they are not the key must-have field for effective execution.
* D. "Risk financial impact" is important for prioritization and cost-benefit analysis, but without an owner, nothing guarantees action.
This is consistent with CRISC's treatment-plan guidance that risk treatment plans "primarily specify the responsibility for implementing the chosen risk treatment and provide treatment for identified risk that exceeds risk tolerance."

NEW QUESTION: 515
The GREATEST benefit of introducing continuous monitoring to an IT control environment is that it:
A. Enables timely detection of emerging risk
B. Enables the collection of benchmarking data
C. Identifies stakeholders involved in the process
D. Helps to obtain buy-in for future IT investments
Answer: A (LEAVE A REPLY)
Continuous monitoring systems automatically track key control indicators (KCIs) and risk metrics in real-time, enabling early identification of anomalies or emerging risks.
ISACA CRISC states:
"Continuous monitoring allows the enterprise to identify deviations and emerging risk conditions in a timely manner to take proactive corrective actions." Benchmarking and stakeholder mapping are secondary benefits.
Thus, A. Enables timely detection of emerging risk is correct.
CRISC Reference: Domain 4 - Risk and Control Monitoring and Reporting, Topic: Continuous Monitoring Benefits.

NEW QUESTION: 516

An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

A. Invoke the incident response plan.

B. Determine the business impact.

C. Conduct a forensic investigation.

D. Invoke the business continuity plan (BCP).

Answer: (SHOW ANSWER)

The first course of action for an organization that has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data is to invoke the incident response plan. An incident response plan is a set of procedures and guidelines that defines the roles and responsibilities of the incident response team, the communication and escalation channels, the incident identification and classification criteria, the incident containment and eradication strategies, the incident recovery and restoration activities, and the incident documentation and reporting requirements. Invoking the incident response plan as soon as possible is crucial to minimize the damage and disruption caused by the cybercrime, to preserve the evidence and facilitate the investigation, and to comply with the legal and regulatory obligations. The other options are not the first course of action, although they may be subsequent or concurrent steps in the incident response process. Determining the business impact is a part of the incident assessment and prioritization phase, which helps to evaluate the severity and scope of the incident and to allocate the appropriate resources and actions. Conducting a forensic investigation is a part of the incident analysis and evidence collection phase, which helps to identify the source and cause of the incident and to support the legal and disciplinary actions. Invoking the business continuity plan (BCP) is a part of the incident recovery and restoration phase, which helps to resume the normal operations and services and to mitigate the adverse effects of the incident. References = The National Cyber Incident Response Plan (NCIRP), Cyber Incident Response Plan | Cyber.gov.au, [Cyber Incident Response: A Framework for Preparation and Success], [Cyber Incident Response Plan: How to Create One for Your Business]

NEW QUESTION: 517

Which of the following is the BEST approach for determining whether a risk action plan is effective?

A. Comparing the remediation cost against budget

B. Assessing changes in residual risk

C. Assessing the inherent risk

D. Monitoring changes of key performance indicators(KPIs)

Answer: (SHOW ANSWER)

According to the CRISC Review Manual (Digital Version), assessing changes in residual risk is the best approach for determining whether a risk action plan is effective, as it measures the impact and value of the risk response actions and controls on the risk level. Residual risk is the risk that remains after the risk response actions and controls have been implemented. Assessing changes in residual risk helps to: Evaluate the extent to which the risk response actions and controls have reduced the likelihood and/or impact of the risk to an acceptable level Identify and report any deviations, errors, or weaknesses in the risk response actions and controls and their performance Recommend and implement corrective actions or improvement measures to address any issues or deficiencies in the risk response actions and controls

Monitor and measure the effectiveness and efficiency of the risk response actions and controls and their alignment with the organization's risk appetite and risk tolerance Update the risk register and the risk treatment plan to reflect the current risk status and the residual risk levels References = CRISC Review Manual (Digital Version), Chapter 3: IT Risk Response, Section 3.2: Risk Response Process, pp. 161-1621

NEW QUESTION: 518
Winch of the following is the BEST evidence of an effective risk treatment plan?
A. The inherent risk is below the asset residual risk.
B. Remediation cost is below the asset business value
C. The risk tolerance threshold s above the asset residual
D. Remediation is completed within the asset recovery time objective (RTO)
Answer: (SHOW ANSWER)
The best evidence of an effective risk treatment plan is that the risk tolerance threshold is above the asset residual risk, because this means that the risk treatment plan has reduced the risk to a level that is acceptable to the enterprise. The risk tolerance threshold is the maximum amount of risk that the enterprise is willing to accept for a given asset or process. The asset residual risk is the remaining risk after applying the risk treatment plan. The risk treatment plan is effective if the asset residual risk is lower than or equal to the risk tolerance threshold. The other options are not the best evidence, although they may also be indicators of an effective risk treatment plan. The inherent risk being below the asset residual risk, the remediation cost being below the asset business value, and the remediation being completed within the asset recovery time objective (RTO) are examples of desirable or expected outcomes of the risk treatment plan, but they do not directly measure the effectiveness of the risk treatment plan. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 519
Which of the following is the MOST critical consideration when awarding a project to a third-party service provider whose servers are located offshore?
A. Cost implications due to installation of network intrusion detection systems (IDSs)
B. Delays in incident communication
C. Potential impact on data governance
D. Difficulty of monitoring compliance due to geographical distance
Answer: (SHOW ANSWER)

NEW QUESTION: 520
Which of the following is the MOST important benefit of implementing a data classification program?
A. Reduction in data complexity
B. Reduction in processing times
C. Identification of appropriate ownership
D. Identification of appropriate controls
Answer: (SHOW ANSWER)

A data classification program helpsidentify appropriate controlsby categorizing data based on sensitivity and criticality. This ensures that data protection measures are aligned with its value and risk level, improving overall security posture.

NEW QUESTION: 521
Which role is primarily responsible for ensuring that business processes are aligned with organizational objectives and that risks related to business operations are managed effectively?
A. Business information security officer
B. Service level manager
C. Business process manager
D. Data center operations manager
Answer: (SHOW ANSWER)
The business process manager is best suited to own business continuity controls because they have direct responsibility for the continuity of the business process and understand the criticality of maintaining operations during disruptions. While security officers and operations managers have important roles, the business process manager is accountable for ensuring the process continues to meet business objectives and should lead continuity efforts#5:513, 5:514 CRISC_SentenceinNOTE30.pptx#.

NEW QUESTION: 522
Who is accountable for the process when an IT stakeholder operates a key control to address a risk scenario?
A. Data custodian
B. Risk owner
C. System owner
D. IT manager
Answer: (SHOW ANSWER)
The risk owner is accountable for managing risk, including overseeing controls addressing identified risk scenarios, regardless of who operates them.
Reference:CRISC Manual - Domain 1: Governance, Slide 82

NEW QUESTION: 523
Which of the following should be considered FIRST when creating a comprehensive IT risk register?
A. Risk management budget
B. Risk mitigation policies
C. Risk appetite
D. Risk analysis techniques
Answer: (SHOW ANSWER)
Risk appetite is the most important factor to consider first when creating a comprehensive IT risk register, as it defines the amount and type of risk that the organization is willing to accept in pursuit of its objectives, and guides the identification, assessment, response, and monitoring of the IT risks. The other options are not the most important factors, as they are more related to the resources, actions, or methods of the IT risk

management, respectively, rather than the strategy or direction of the IT risk management. References = CRISC Review Manual, 7th Edition, page 109.

NEW QUESTION: 524
An organization's IT team has proposed the adoption of cloud computing as a cost-saving measure for the business. Which of the following should be of GREATEST concern to the risk practitioner?
A. Due diligence for the recommended cloud vendor has not been performed.
B. The business can introduce new Software as a Service (SaaS) solutions without IT approval.
C. The maintenance of IT infrastructure has been outsourced to an Infrastructure as a Service (IaaS) provider.
D. Architecture responsibilities may not be clearly defined.
Answer: A (LEAVE A REPLY)
The lack of due diligence for the recommended cloud vendor should be of greatest concern to the risk practitioner, because it exposes the organization to potential risks and issues related to the security, reliability, performance, and compliance of the cloud service provider. Due diligence is a process of conducting a thorough investigation and evaluation of a potential vendor or partner before entering into a contractual relationship. Due diligence helps to verify the vendor's credentials, capabilities, reputation, and track record, and to identify any red flags or gaps that may affect the quality or suitability of the service.
Cloud computing is a model of delivering IT services over the internet, where the service provider owns and manages the IT infrastructure, platforms, or applications, and the customer pays only for the resources or functions they use.
Cloud computing can offer cost savings, scalability, and flexibility for the business, but it also introduces new risks and challenges, such as data privacy, security breaches, vendor lock-in, service outages, or regulatory compliance. Therefore, performing due diligence for the recommended cloud vendor is essential to ensure that the organization's expectations and requirements are met, and that the risks and issues are identified and addressed. The business introducing new SaaS solutions without IT approval, the maintenance of IT infrastructure being outsourced to an IaaS provider, and the architecture responsibilities not being clearly defined are all possible concerns for the risk practitioner, but they are not the greatest concern, as they can be mitigated or resolved with appropriate controls, policies, or agreements. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.2.1, page 183

NEW QUESTION: 525
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?
A. Complete an offsite business continuity exercise.
B. Conduct a compliance check against standards.
C. Perform a vulnerability assessment.
D. Measure the change in inherent risk.
Answer: (SHOW ANSWER)
A business system is a set of interconnected processes, functions, or activities that support the operations and objectives of a business1. A security gap is a weakness or flaw in a business system that can be

exploited by a threat to cause harm or gain unauthorized access2. A control is a measure or mechanism that reduces the likelihood or impact of a security gap or threat3.
The best way to determine whether new controls mitigate security gaps in a business system is to perform a vulnerability assessment. A vulnerability assessment is a process of identifying and evaluating the security gaps and threats in a business system, and testing the effectiveness and efficiency of the controls that are implemented to address them. A vulnerability assessment can help to:
Measure and compare the current and desired state of the security posture and performance of the business system Detect and prioritize the most critical and urgent security gaps and threats that may compromise the business system or its objectives Validate and validate the adequacy and reliability of the new controls and their ability to prevent, detect, or respond to security incidents or breaches Provide feedback and recommendations for improving the security of the business system and enhancing the security awareness and culture of the organization References = What is a Business System?, What is a Security Gap?, What is a Control?, [What is a Vulnerability Assessment?], [Vulnerability Assessment: A Guide for Business Leaders]

NEW QUESTION: 526
An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?
A. Audit reports
B. Industry benchmarks
C. Financial forecasts
D. Annual threat reports
Answer: (SHOW ANSWER)
The best input for conducting a review of emerging risk is the annual threat reports. Emerging risk is the risk that arises from new or evolving sources, or from existing sources that have not been previously considered or recognized. Emerging risk may have significant impact on the organization's objectives, strategies, operations, or reputation, and may require new or different risk responses. Annual threat reports are the reports that provide information and analysis on the current and future trends, developments, and challenges in the threat landscape, such as cyberattacks, natural disasters, geopolitical conflicts, or pandemics. Annual threat reports can help to identify and assess the emerging risk, as they can provide insights into the sources, drivers, indicators, and scenarios of the emerging risk, as well as the potential impact and likelihood of the emerging risk. Annual threat reports can also help to benchmark and compare the organization's risk exposure and preparedness with the industry and the peers, and to prioritize and respond to the emerging risk. Audit reports, industry benchmarks, and financial forecasts are not as useful as annual threat reports, as they do not focus on the emerging risk, and may not capture the latest or future changes in the threat landscape. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 50.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here:

https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 527
Which of the following outcomes of disaster recovery planning is MOST important to enable the initiation of necessary actions during a disaster?
A. Definition of disaster recovery plan (DRP) scope and key stakeholders
B. Recovery time and maximum acceptable data loss thresholds
C. A checklist including equipment, location of data backups, and backup sites
D. A list of business areas and critical functions subject to risk analysis
Answer: (SHOW ANSWER)
Defining recovery time objectives (RTOs) and acceptable data loss thresholds is critical for effective disaster response, ensuring recovery activities are aligned with business priorities. This supports Business Continuity Planning.

NEW QUESTION: 528
Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?
A. Segregation of duties
B. Three lines of defense
C. Compliance review
D. Quality assurance review
Answer: (SHOW ANSWER)
The three lines of defense model is a framework that defines the roles and responsibilities of different functions in an organization for managing risks and ensuring effective internal control1. The three lines of defense are:
The first line of defense: the operational management and staff who are responsible for implementing and maintaining the internal control system and managing the risks within their areas of activity The second line of defense: the oversight functions, such as risk management, compliance, and quality assurance, who provide guidance, support, and monitoring to the first line of defense and ensure that the internal control system is designed and operating effectively The third line of defense: the internal audit function, who provides independent and objective assurance to the board and senior management on the adequacy and effectiveness of the internal control system and the performance of the first and second lines of defense2
The three lines of defense model facilitates a completely independent review of test results for evaluating control effectiveness, because it ensures that the internal audit function, as the third line of defense, has the authority, independence, and competence to conduct objective and unbiased assessments of the internal control system and report its findings and recommendations to the board and senior management3. The internal audit function can also use the test results from the first and second lines of defense as inputs for its own audit planning and testing, and verify their validity and reliability4.

References = The Three Lines of Defense in Effective Risk Management and Control - IIA, The Three Lines Model - IIA, The Role of Internal Audit in the Three Lines of Defense - IIA, Evaluating and Improving Internal Control in Organizations - IFAC

NEW QUESTION: 529
Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?
A. Senior management
B. Project manager
C. Project sponsor
D. IT risk manager
Answer: (SHOW ANSWER)
A project sponsor is the person or group who provides the financial, political, or organizational support for a project, and who has the authority to approve or reject the project's objectives, scope, budget, schedule, and deliverables.
The primary recipient of reports showing the progress of a current IT risk mitigation project should be the project sponsor, because they are ultimately responsible for the success or failure of the project, and they need to be informed of the project's status, issues, risks, and achievements on a regular basis.
The other options are not the primary recipients of reports showing the progress of a current IT risk mitigation project. They are either secondary or not essential for project reporting.
The references for this answer are:
Risk IT Framework, page 21
Information Technology & Security, page 15
Risk Scenarios Starter Pack, page 13

NEW QUESTION: 530
Which of the following provides the MOST comprehensive information when developing a risk profile for a system?
FreeCram.net
A. Results of a business impact analysis (BIA)
B. Risk assessment results
C. A mapping of resources to business processes
D. Key performance indicators (KPIs)
Answer: (SHOW ANSWER)
The most comprehensive information for developing a risk profile for a system is the risk assessment results. A risk assessment is a process that identifies, analyzes, and evaluates the risks that could affect the system's objectives or operations. A risk assessment provides comprehensive information for developing a risk profile, because it helps to determine the likelihood and impact of the risks, and to prioritize them based on their severity and relevance. A risk assessment also helps to select the most appropriate and effective controls to minimize the risks, such as avoiding, reducing, transferring, or accepting the risks. A risk profile is a document that summarizes the key risks that the system faces or accepts, and their likelihood, impact, and priority. A risk profile helps to identify and prioritize the most critical or relevant risks, and to align them with

the system's objectives, strategy, and risk appetite. The other options are not as comprehensive as the risk assessment results, although they may be part of or derived from the risk profile. Results of a business impact analysis (BIA), a mapping of resources to business processes, and key performance indicators (KPIs) are all factors that could affect the system's performance and improvement, but they do not necessarily identify, analyze, or evaluate the risks that could affect the system. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 531
Of the following, whose input is ESSENTIAL when developing risk scenarios for the implementation of a third-party mobile application that stores customer data?
A. Business process owner
B. IT compliance manager
C. IT vendor manager
D. Information security manager
Answer: (SHOW ANSWER)

NEW QUESTION: 532
An organization has committed to a business initiative with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?
A. Recommend rejection of the initiative.
B. Change the level of risk appetite.
C. Document formal acceptance of the risk.
D. Initiate a reassessment of the risk.
Answer: C (LEAVE A REPLY)
Formal acceptance of the risk is critical when the risk exposure exceeds the risk appetite, as it ensures accountability and acknowledges the decision at the appropriate level. Documenting acceptance involves communicating the potential impacts and obtaining agreement from senior stakeholders. This process aligns with theRisk Response and Reportingdomain in CRISC, emphasizing clear documentation and communication of risks for decision-making.

NEW QUESTION: 533
Which of the following BEST helps to identify significant events that could impact an organization?
A. Control analysis
B. Vulnerability analysis
C. Scenario analysis
D. Heat map analysis
Answer: (SHOW ANSWER)
Scenario analysis is the best method to identify significant events that could impact an organization. Scenario analysis is the process of creating and evaluating hypothetical situations or scenarios that represent plausible outcomes of various events or actions. Scenario analysis helps to anticipate and prepare for

potential risks and opportunities, as well as to test the robustness and resilience of the organization's strategies and plans. Control analysis, vulnerability analysis, and heat map analysis are not as effective as scenario analysis, because they focus on the existing or current state of the organization, rather than the future or alternative states. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 534
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?
A. Data classification policy
B. Emerging technology trends
C. The IT strategic plan
D. The risk register
Answer: (SHOW ANSWER)
The most comprehensive resource for prioritizing the implementation of information systems controls is the risk register. The risk register is a document that records the identified risks, their analysis, and their responses. The risk register provides a holistic and systematic view of the risk profile and the risk treatment of the organization. The risk register can help to prioritize the implementation of information systems controls by providing the information on the likelihood, impact, and exposure of the risks, the effectiveness and efficiency of the controls, and the gaps or issues of the control environment. The other options are not as comprehensive as the risk register, as they are related to the specific aspects or components of the information systems controls, not the overall assessment and evaluation of the information systems controls. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.4: IT Risk Response, page 87.

NEW QUESTION: 535
Read" rights to application files in a controlled server environment should be approved by the:
A. business process owner.
B. database administrator.
C. chief information officer.
D. systems administrator.
Answer: (SHOW ANSWER)
Read rights: The permission to view or access the content of a file or a folder1.
Application files: The files that contain the code, data, or resources of an application or a program2.
Controlled server environment: A server environment that is managed and secured by a set of policies, procedures, and tools3.
Business process owner: The person who is responsible for the design, execution, and performance of a business process.
Read rights to application files in a controlled server environment should be approved by the business process owner. The business process owner is the person who has the authority and accountability for the

business process that uses or depends on the application files. The business process owner should approve the read rights to application files in a controlled server environment to:
Ensure that the read rights are aligned with the business needs and objectives Prevent unauthorized or unnecessary access to the application files Protect the confidentiality, integrity, and availability of the application files Comply with the relevant laws and regulations that govern the access to the application files The other options are not the best choices for approving the read rights to application files in a controlled server environment, because they do not have the same level of authority, responsibility, or knowledge as the business process owner. The database administrator, who is the person who manages and maintains the database systems and data, may have the technical skills and access to grant the read rights to application files, but they may not have the business insight or approval to do so. The chief information officer, who is the person who oversees the IT strategy and operations of the organization, may have the executive power and oversight to approve the read rights to application files, but they may not have the specific or detailed knowledge of the business process or the application files. The systems administrator, who is the person who configures and maintains the server systems and networks, may have the administrative privileges and tools to grant the read rights to application files, but they may not have the business understanding or authorization to do so.
References = Read Permission - an overview | ScienceDirect Topics, What is an Application File? - Definition from Techopedia, What is a Server Environment? - Definition from Techopedia, [Business Process Owner: Definition, Roles, and Responsibilities]

NEW QUESTION: 536
Which of the following is the MOST effective way to help ensure future risk levels do not exceed the organization's risk appetite?
A. Developing contingency plans for key processes
B. Implementing key performance indicators (KPIs)
C. Adding risk triggers to entries in the risk register
D. Establishing a series of key risk indicators (KRIs)
Answer: (SHOW ANSWER)
Key Risk Indicators (KRIs)are metrics used to monitor changes in risk exposure, enabling proactive adjustments to keep risks within appetite. They provide early warnings of potential breaches in risk thresholds.

NEW QUESTION: 537
A risk practitioner is advising management on how to update the IT policy framework to account for the organization s cloud usage. Which of the following should be the FIRST step in this process?
A. Consult with industry peers regarding cloud best practices.
B. Evaluate adherence to existing IT policies and standards.
C. Determine gaps between the current state and target framework.
D. Adopt an industry-leading cloud computing framework.
Answer: (SHOW ANSWER)
Updating IT Policy Framework for Cloud Usage:

Gap Analysis: The first step in updating the IT policy framework is to conduct a gap analysis to identify discrepancies between the current state and the desired target framework for cloud usage.
Assessment of Current State: This involves reviewing existing policies, controls, and practices related to cloud usage to understand current capabilities and limitations.
Target Framework Definition: Define the desired state based on industry best practices, regulatory requirements, and organizational objectives.
Importance of Gap Analysis:
Focused Improvements: Identifying gaps allows the organization to focus on specific areas that need enhancement to align with best practices and compliance requirements.
Resource Allocation: Helps in allocating resources effectively to address the most critical gaps first.
Comparison with Other Options:
Consult with Industry Peers: Useful for gathering insights but should follow the gap analysis to ensure relevance to the organization's specific context.
Evaluate Adherence to Existing Policies: Part of the gap analysis but not the initial step.
Adopt Industry-leading Framework: Important for long-term strategy but should be based on identified gaps.
Best Practices:
Comprehensive Review: Conduct a thorough review of existing policies and compare them with industry standards.
Stakeholder Involvement: Engage relevant stakeholders in the gap analysis to ensure all perspectives are considered.
References:
CRISC Review Manual: Emphasizes the importance of gap analysis in aligning IT policies with cloud computing frameworks and best practices .
ISACA Guidelines: Recommend conducting gap analysis as a foundational step in updating IT policy frameworks to ensure comprehensive and effective cloud governance .

NEW QUESTION: 538
The BEST way to demonstrate alignment of the risk profile with business objectives is through:
A. risk scenarios.
B. risk tolerance.
C. risk policy.
D. risk appetite.
Answer: (SHOW ANSWER)
The BEST way to demonstrate alignment of the risk profile with business objectives is through risk scenarios, because they are the descriptions and illustrations of the potential events or situations that may affect the achievement of the business objectives and processes. Risk scenarios can help to demonstrate how the risk profile, which is the summary and representation of the identified and assessed risks, is related and relevant to the business objectives and processes, and how the risk responses and controls are designed and implemented to support and enable the business objectives and processes. The other options are not the best way, because:

* Option B: Risk tolerance is the level of variation or deviation from the expected or desired outcome that the organization is willing to accept or endure, but it does not demonstrate alignment of the risk profile with business objectives, which is the process of ensuring that the risk profile and the business objectives are consistent and compatible with each other.
* Option C: Risk policy is the document that defines the principles, guidelines, and requirements for the risk management process and activities in the organization, but it does not demonstrate alignment of the risk profile with business objectives, which is the process of showing and proving that the risk profile and the business objectives are coherent and integrated with each other.
* Option D: Risk appetite is the amount and type of risk that the organization is willing to take or pursue in order to achieve its objectives and goals, but it does not demonstrate alignment of the risk profile with business objectives, which is the process of establishing and maintaining that the risk profile and the business objectives are aligned and balanced with each other. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 104.

NEW QUESTION: 539
A legacy application used for a critical business function relies on software that has reached the end of extended support Which of the following is the MOST effective control to manage this application?
A. Subscribe to threat intelligence to monitor external attacks.
B. Apply patches for a newer version of the application.
C. Segment the application within the existing network.
D. Increase the frequency of regular system and data backups.
Answer: C (LEAVE A REPLY)
Segmenting the application within the existing network is the most effective control to manage a legacy application that relies on software that has reached the end of extended support, as it isolates the application from the rest of the network and reduces the attack surface and the potential impact of a compromise. Subscribing to threat intelligence, applying patches for a newer version of the application, and increasing the frequency of regular system and data backups are not the most effective controls, as they may not address the root cause of the risk, or may introduce additional costs or complexities, respectively. References = CRISC Review Manual, 7th Edition, page 153.

NEW QUESTION: 540
Which of the following is the PRIMARY benefit of implementing key control indicators (KCIs)?
A. Confirming the adequacy of recovery plans.
B. Improving compliance with control standards.
C. Providing early detection of control degradation.
D. Reducing the number of incidents.
Answer: (SHOW ANSWER)
Key Control Indicators (KCIs) are metrics used to monitor the performance of controls. Their primary benefit is the early detection of control degradation, allowing organizations to take corrective actions before issues escalate into significant problems.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 3: Risk Response and Reporting, Section:

Control Monitoring and Reporting.

NEW QUESTION: 541
Which of the following is the BEST key performance indicator (KPI) to measure the ability to deliver uninterrupted IT services?
A. Mean time between failures (MTBF)
B. Mean time to recover (MTTR)
C. Planned downtime
D. Unplanned downtime
Answer: (SHOW ANSWER)
Mean time between failures (MTBF) is a key performance indicator (KPI) that measures the average time that a system or component operates without interruption or failure. MTBF is a common metric for reliability and availability of IT services. A higher MTBF indicates a lower frequency of failures and a higher ability to deliver uninterrupted IT services. According to the CRISC Review Manual 2022, MTBF is one of the KPIs for IT service delivery1. According to the CRISC Review Questions, Answers & Explanations Manual 2022, MTBF is the correct answer to this question2.
Mean time to recover (MTTR), planned downtime, and unplanned downtime are not the best KPIs to measure the ability to deliver uninterrupted IT services. MTTR measures the average time that it takes to restore a system or component to normal operation after a failure. Planned downtime measures the scheduled time that a system or component is not available for use due to maintenance or upgrades. Unplanned downtime measures the unscheduled time that a system or component is not available for use due to failures or incidents.
These KPIs are useful for measuring the impact and duration of service interruptions, but they do not directly reflect the ability to prevent or avoid service interruptions.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 542
An online retailer has decided to store its customer database with a cloud provider in an Infrastructure as a Service (IaaS) configuration. During an initial review of preliminary risk scenarios, a risk practitioner identifies instances where sensitive customer information is stored unencrypted. Who is accountable for ensuring this encryption?
A. The retailer's IT department
B. The chief information officer (CIO)
C. The data owner

D. The cloud provider
Answer: (SHOW ANSWER)

NEW QUESTION: 543
Which of the following should be done FIRST when developing an initial set of risk scenarios for an organization?
A. Use a top-down approach.
B. Consider relevant business activities.
C. Refer to industry standard scenarios.
D. Use a bottom-up approach.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 544
During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:
A. compensating controls are in place.
B. a control mitigation plan is in place.
C. risk management is effective.
D. residual risk is accepted.
Answer: A (LEAVE A REPLY)
Compensating controls are additional or alternative controls that are implemented when the existing controls are found to be ineffective or do not meet the required standards. Compensating controls are designed to reduce the risk exposure to an acceptable level and ensure that the organization can still comply with the relevant regulations and industry best practices. For an organization that processes credit cards, compensating controls may include enhanced encryption, monitoring, auditing, or authentication mechanisms. By having compensating controls in place, the organization can maintain an effective overall control environment despitethe deficiencies in the existing controls. The other options are not correct because they do not ensure that the overall control environment is effective. A control mitigation plan is a document that outlines the actions and resources needed to address the control deficiencies, but it does not guarantee that the compensating controls will be implemented or effective. Risk management is a process that involves identifying, analyzing, evaluating, and treating risks, but it does not directly affect the control environment. Residual risk is the risk that remains after the risk treatment, and it may or may not be acceptable depending on the risk appetite of the organization. References = CRISC Review Manual, pages 153-1541; CRISC Review Questions, Answers & Explanations Manual, page 632

NEW QUESTION: 545
Well-developed, data-driven risk measurements should be:
A. reflective of the lowest organizational level.
B. a data feed taken directly from operational production systems.
C. reported to management the same day data is collected.

D. focused on providing a forward-looking view.

Answer: (SHOW ANSWER)

Well-developed, data-driven risk measurements should be focused on providing a forward-looking view, as they enable the organization to anticipate and prepare for the potential changes and impacts of the risk level and exposure, and to take proactive and appropriate actions to address the risk. The other options are not the characteristics of well-developed, data-driven risk measurements, as they may not reflect the strategic, comprehensive, or timely aspects of the risk measurements, respectively. References = CRISC Review Manual, 7th Edition, page 110.

NEW QUESTION: 546

Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?

A. Adopting qualitative enterprise risk assessment methods

B. Linking IT risk scenarios to technology objectives

C. linking IT risk scenarios to enterprise strategy

D. Adopting quantitative enterprise risk assessment methods

Answer: (SHOW ANSWER)

The best way to facilitate the alignment of IT risk management with enterprise risk management (ERM) is to link IT risk scenarios to enterprise strategy, because this ensures that the IT risks are considered in the context of the enterprise's mission, vision, and goals. Linking IT risk scenarios to enterprise strategy also helps to prioritize the IT risks based on their impact and relevance to the enterprise's objectives, and to select the appropriate risk responses and resources. The other options are not the best ways to facilitate the alignment of IT risk management with ERM, because they do not address the integration or alignment of the IT and enterprise perspectives. Adopting qualitative or quantitative enterprise risk assessment methods, and linking IT risk scenarios to technology objectives are examples of techniques or tools that can be used to perform IT risk management or ERM, but they do not ensure the alignment or consistency of the two processes. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section
1.2.3, p. 22.

NEW QUESTION: 547

Which of the following is the MOST useful information an organization can obtain from external sources about emerging threats?

A. Solutions for eradicating emerging threats

B. Cost to mitigate the risk resulting from threats

C. Indicators for detecting the presence of threatsl)

D. Source and identity of attackers

Answer: (SHOW ANSWER)

*External sources of emerging threats are sources that provide information about the latest cyberattacks, hacking techniques, malware, and vulnerabilities that can affect an organization's IT systems and data.

Examples of external sources are security blogs, forums, newsletters, reports, and alerts from reputable organizations such as ISACA, Imperva, Aura, and BitSight123.
*The most useful information an organization can obtain from external sources is the indicators for detecting the presence of threats. Indicators are observable signs or patterns that can help identify, prevent, or mitigate cyberattacks. Examples of indicators are IP addresses, domain names, file hashes, network traffic, system logs, and user behavior4.
*Indicators for detecting the presence of threats are more useful than the other options because they can help an organization to:
oMonitor and analyze its IT environment for any suspicious or malicious activity oRespond quickly and effectively to any potential or actual incidents oReduce the impact and damage of cyberattacks oImprove its security posture and resilience
*Solutions for eradicating emerging threats are not the most useful information because they may not be applicable or effective for every organization, depending on its specific context, needs, and resources. Moreover, solutions may not be available or known for some new or sophisticated threats.
*Cost to mitigate the risk resulting from threats is not the most useful information because it does not help an organization to identify or prevent cyberattacks. Cost is only one factor to consider when deciding how to manage IT risk, and it may not reflect the true value or impact of the threats.
*Source and identity of attackers are not the most useful information because they may not be relevant or accurate for every organization. Source and identity of attackers are often difficult to trace or verify, and they may not affect the organization's risk level or response strategy.
References =
*Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, Chapter 2: IT Risk Assessment, Section 2.3: Risk Identification, pp. 83-84
*Risk and Information Systems Control Review Questions, Answers & Explanations Database, 12 Month Subscription, ISACA, 2020, Question ID: 100000

NEW QUESTION: 548
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?
A. Financial risk is given a higher priority.
B. Risk with strategic impact is included.
C. Security strategy is given a higher priority.
D. Risk identified by industry benchmarking is included.
Answer: (SHOW ANSWER)
According to the ISACA CRISC Review Manual, an enterprise risk management (ERM) process is a holistic approach to identifying, analyzing, responding to, and monitoring all types of risk that affect the achievement of the enterprise's objectives. The ERM process should consider all types of risk, including strategic, operational, financial, compliance, and reputational risks. Among these, strategic risks are the most important, as they have the potential to affect the enterprise's mission, vision, and goals. Therefore, risk with strategic impact should be included in the ERM process. References = ISACA CRISC Review Manual, 7th Edition, Chapter 1, Section 1.2.1, page 17.

NEW QUESTION: 549
Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?
A. Perform a gap analysis
B. Conduct system testing
C. Implement compensating controls
D. Update security policies
Answer: (SHOW ANSWER)
Performing a gap analysis is the best recommendation for a risk practitioner upon learning of an updated cybersecurity regulation that could impact the organization. A gap analysis can help identify the current state of compliance, the desired state of compliance, and the actions needed to achieve compliance. Conducting system testing, implementing compensating controls, and updating security policies are possible actions that may result from the gap analysis, but they are not the best initial recommendation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 1; CRISC Review Manual, 6th Edition, page 143.

NEW QUESTION: 550
Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?
Freecram.net
A. Quantitative analysis might not be possible.
B. Risk factors might not be relevant to the organization
C. Implementation costs might increase.
D. Inherent risk might not be considered.
Answer: (SHOW ANSWER)
According to the CRISC 351-400 topic3 Flashcards, the greatest concern when using a generic set of IT risk scenarios for risk analysis is that the risk factors might not be relevant to the organization. This is because generic risk scenarios are not tailored to the specific context, objectives, and environment of the organization, and they may not capture the unique threats, vulnerabilities, and impacts that the organization faces.
Therefore, using generic risk scenarios may result in inaccurate or incomplete risk assessment and analysis, and may lead to ineffective or inappropriate risk responses. To avoid this, the organization should customize the risk scenarios to reflect its own situation and needs, and involve the relevant stakeholders and experts in the process. References = CRISC 351-400 topic3 Flashcards, Generic IT Risk Scenarios for Risk Analysis: The Greatest Concern

NEW QUESTION: 551
Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?
A. To align with board reporting requirements
B. To assist management in decision making

C. To create organization-wide risk awareness
D. To minimize risk mitigation efforts
Answer: (SHOW ANSWER)
Risk tolerance and appetite are the expressions of the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk tolerance is the acceptable level of variation that the organization is willing to allow for the outcome of its risk decisions. Risk appetite is the broad-based amount of risk that the organization is willing to accept in its activities. The primary objective of establishing an organization's risk tolerance and appetite is to assist management in decision making, as they provide guidance and boundaries for the risk management activities and decisions. By establishing the risk tolerance and appetite, the organization can align its risk exposure with its strategic goals, optimize its risk-return trade-off, and enhance its risk culture and performance. References = CRISC Review Manual, 7th Edition, page 61.

NEW QUESTION: 552
The annualized loss expectancy (ALE) method of risk analysis:
A. helps in calculating the expected cost of controls
B. uses qualitative risk rankings such as low. medium and high.
C. can be used m a cost-benefit analysts
D. can be used to determine the indirect business impact.
Answer: (SHOW ANSWER)
The annualized loss expectancy (ALE) method of risk analysis is a quantitative method that estimates the expected monetary loss that can result from a risk over a one year period. The ALE is calculated by multiplying the single loss expectancy (SLE), which is the monetary loss from a single occurrence of a risk, by the annualized rate of occurrence (ARO), which is the frequency of the risk occurring in a year. The ALE can be used in a cost-benefit analysis to compare the cost of implementing a control or a risk response with the expected benefit of reducing the loss. The ALE can help to justify the investment in risk management and to prioritize the risks based on their financial impact. The other options are not accurate descriptions of the ALE method of risk analysis, as they involve different aspects or methods of risk analysis. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.3.2.1, pp. 60-61.

NEW QUESTION: 553
Which of the following is the MOST effective control to maintain the integrity of system configuration files?
A. Recording changes to configuration files
B. Implementing automated vulnerability scanning
C. Restricting access to configuration documentation
D. Monitoring against the configuration standard
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, monitoring against the configuration standard is the most effective control to maintain the integrity of system configuration files, because it ensures that any unauthorized or unintended changes are detected and corrected. Monitoring against the configuration standard involves comparing the actual configuration of the system with the approved baseline and identifying any deviations or discrepancies. The other options are not the most effective controls, because they do not ensure the integrity

of the system configuration files. Recording changes to configuration files is a good practice, but it does not prevent unauthorized or unintended changes from occurring. Implementing automated vulnerability scanning is a preventive control that helps to identify and remediate potential weaknesses in the system, but it does not verify the integrity of the configuration files. Restricting access to configuration documentation is a security measure that limits the exposure of sensitive information, but it does not prevent unauthorized or unintended changes to the configuration files. References = CRISC Review Manual, 7th Edition, Chapter 4, Section 4.2.3, page 184.

NEW QUESTION: 554
Which of the following is the BEST method for assessing control effectiveness?
A. Ad hoc control reporting
B. Control self-assessment
C. Continuous monitoring
D. Predictive analytics
Answer: (SHOW ANSWER)
Control effectiveness is the degree to which a control achieves its intended objective and mitigates the risk that it is designed to address. It is measured by comparing the actual performance and outcome of the control with the expected or desired performance and outcome.
The best method for assessing control effectiveness is continuous monitoring, which is the process of collecting, analyzing, and reporting on the performance and outcome of the controls on an ongoing basis. Continuous monitoring provides timely and accurate information on the status and results of the controls, and enables the identification and correction of any issues or gaps in the control environment.
Continuous monitoring can be performed using various techniques, such as automated tools, dashboards, indicators, metrics, logs, audits, reviews, etc. Continuous monitoring can also be integrated with the risk management process, and aligned with the organization's objectives and risk appetite.
The other options are not the best methods for assessing control effectiveness, because they do not provide the same level of timeliness, accuracy, and completeness of information on the performance and outcome of the controls.
Ad hoc control reporting is the process of collecting, analyzing, and reporting on the performance and outcome of the controls on an irregular or occasional basis. Ad hoc control reporting may be triggered by specific events, requests, or incidents, and it may not cover all the relevant or critical controls. Ad hoc control reporting may not provide sufficient or consistent information on the control effectiveness, and it may not enable the timely and proactive identification and correction of any issues or gaps in the control environment.
Control self-assessment is the process of allowing the control owners or operators to evaluate and report on the performance and outcome of their own controls. Control self-assessment can provide useful insights and feedback from the control owners or operators, and it can enhance their awareness and accountability for the control effectiveness. However, control self-assessment may not be objective, reliable, or independent, and it may not cover all the relevant or critical controls. Control self-assessment may not provide sufficient or consistent information on the control effectiveness, and it may not enable the timely and proactive identification and correction of any issues or gaps in the control environment.

Predictive analytics is the process of using statistical techniques and models to analyze historical and current data, and to make predictions or forecasts about future events or outcomes. Predictive analytics can provide useful insights and trends on the potential performance and outcome of the controls, and it can support the decision making and planning for the control effectiveness. However, predictive analytics may not be accurate, valid, or reliable, and it may not reflect the actual or current performance and outcome of the controls. Predictive analytics may not provide sufficient or consistent information on the control effectiveness, and it may not enable the timely and proactive identification and correction of any issues or gaps in the control environment. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 40-41, 47-48, 54-55, 58-59, 62-63 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 150 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 555
Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?
A. Expertise in both methodologies
B. Maturity of the risk management program
C. Time available for risk analysis
D. Resources available for data analysis
Answer: C (LEAVE A REPLY)
The most important consideration when selecting either a qualitative or quantitative risk analysis is the time available for risk analysis, as this affects the level of detail and accuracy that can be achieved in the risk assessment process. Qualitative risk analysis is a method that uses subjective judgments and ratings to measure and prioritize the risks based on their likelihood and impact, as well as other factors such as urgency, velocity, and persistence. Qualitative risk analysis is usually faster and simpler than quantitative risk analysis, but it may also be less precise and consistent. Quantitative risk analysis is a method that uses numerical data and mathematical models to measure and prioritize the risks based on theirprobability and magnitude, as well as other factors such as frequency, duration, and correlation. Quantitative risk analysis is usually more complex and time-consuming than qualitative risk analysis, but it may also provide more objective and reliable results. The other options are not the most important considerations when selecting either a qualitative or quantitative risk analysis, although they may have some influence or relevance. Expertise in both methodologies is desirable, but it does not determine the choice of the risk analysis method, as it depends on the availability and suitability of the experts for the specific risk context and objectives. Maturity of the risk management program is important, but it does not dictate the choice of the risk analysis method, as it depends on the level of integration and alignment of the risk management activities with the enterprise's strategy and goals. Resources available for data analysis are relevant, but they do not decide the choice of the risk analysis method, as they depend on the quality and availability of the data sources and tools for the risk assessment process. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Assessment, page 81.ST

NEW QUESTION: 556
Which of the following indicates an organization follows IT risk management best practice?

A. The risk register template uses an industry standard.
B. The risk register is regularly updated.
C. All fields in the risk register have been completed.
D. Controls are listed against risk entries in the register.
Answer: (SHOW ANSWER)
According to the IT Risk Management - Basics and Best Practices article, one of the best practices for IT risk management is to keep the risk register up to date. A risk register is a document that records the identified risks, their causes, impacts, likelihood, responses, and status. A risk register is a vital tool for IT risk management, as it helps to track and monitor the risks throughout their lifecycle, and to communicate the risks to the relevant stakeholders. However, a risk register is only useful if it reflects the current situation and environment of the organization. Therefore, the risk register should be regularly updated to capture any changes in the risk profile, such as new risks, resolved risks, modified risks, or escalated risks. Updating the risk register will help to ensure that the risk management process is effective and efficient, and that the risk responses are appropriate and timely. References = IT Risk Management - Basics and Best Practices

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 557
Where should a risk practitioner document the current state and desired future state of organizational risk?
A. Risk action plan
B. Risk management strategy
C. Risk register
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)

NEW QUESTION: 558
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?
A. User access may be restricted by additional security.
B. Unauthorized access may be gained to multiple systems.
C. Security administration may become more complex.
D. User privilege changes may not be recorded.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, single sign-on (SSO) is a method of authentication that allows a user to access multiple systems or applications with a single set of credentials. SSO can improve user

convenience and productivity, but it also introduces some security risks. The greatest concern as a result of a single sign-on implementation is that unauthorized access may be gained to multiple systems, as this can compromise the confidentiality, integrity, and availability of the data and resources stored on those systems. If an attacker obtains the SSO credentials of a user, either by phishing, malware, or other means, they can Laccess all the systems or applications that the user is authorized for, without any additional authentication or verification. This can expose the organization to various threats, such as data leakage, theft, loss, corruption, manipulation, or misuse2345. References = CRISC Review Manual1, page 240, 253.

NEW QUESTION: 559
Which of the following should be given the HIGHEST priority when developing a response plan for risk assessment results?
A. Risk that has been untreated
B. Items with the highest likelihood of occurrence
C. Items with a high inherent risk
D. Risk that exceeds risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 560
Reviewing which of the following BEST helps an organization gain insight into its overall risk profile?
A. Threat landscape
B. Risk appetite
C. Risk register
D. Risk metrics
Answer: (SHOW ANSWER)
Reviewing the risk register is the best way to help an organization gain insight into its overall risk profile, because it provides a comprehensive and structured representation of all the key risks that the organization faces, along with their likelihood, impact, and response strategies. A risk register is a tool that records and tracks the current status of risks, their sources, causes, consequences, and controls. A risk register helps to facilitate the communication and reporting of risks, and to support the risk-based decision making and prioritization. A risk profile is a summary of the key risks that an organization faces, and their implications for the organization's objectives and strategy. Reviewing the risk register is the best way to understand the risk profile, as it reflects the nature and level of exposure that the organization has from the various risk sources and scenarios. Reviewing the threat landscape, the risk appetite, and the risk metrics are all useful ways to help an organization gain insight into its overall risk profile, but they are not the best way, as they do not provide a comprehensive and structured view of the risks and their responses. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.1, page 83

NEW QUESTION: 561
A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?
A. Customer database manager

B. Customer data custodian
C. Data privacy officer
D. Audit committee
Answer: (SHOW ANSWER)
The data privacy officer is the best person to notify in case of a new malware that has severely impacted industry peers with data loss. The data privacy officer is responsible for ensuring that the enterprise complies with the applicable privacy laws and regulations, and that the personal data of the customers, employees, and other stakeholders are protected from unauthorized access, use, disclosure, or destruction. The data privacy officer can assess the potential impact of the malware on the enterprise's data privacy obligations and risks, and coordinate the appropriate response and remediation actions. The customer database manager, the customer data custodian, and the audit committee are not the best persons to notify, as they do not have the same level of authority, responsibility, and expertise as the data privacy officer in dealing with data privacy issues. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 191.

NEW QUESTION: 562
Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?
A. Apply available security patches.
B. Schedule a penetration test.
C. Conduct a business impact analysis (BIA)
D. Perform a vulnerability analysis.
Answer: (SHOW ANSWER)
The best recommendation to address an organization's need to secure multiple systems with limited IT resources is to perform a vulnerability analysis. A vulnerability analysis is a process of identifying, assessing, and prioritizing the weaknesses or flaws in the systems that could be exploited by threats or risks. A vulnerability analysis helps to determine the level and nature of the exposure and impact of the systems, and to select and implement the appropriate security controls or mitigations. Performing a vulnerability analysis is the best recommendation, as it helps to optimize the use of the limited IT resources, by focusing on the most critical or significant vulnerabilities, and by applying the most effective or efficient security solutions. Performing a vulnerability analysis also helps to improve the security posture and performance of the systems, and to reduce the likelihood and consequences of security incidents or breaches. Applying available security patches, scheduling a penetration test, and conducting a business impact analysis (BIA) are not the best recommendations, as they are either the outputs or the inputs of the vulnerability analysis process, and they do not address the primary need of securing the systems with limited IT resources. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 563
Which of the following BEST reduces the likelihood of fraudulent activity that occurs through use of a digital wallet?
A. Require multi-factor authentication (MFA) to access the digital wallet.
B. Use a digital key to encrypt the contents of the wallet.

C. Enable audit logging on the digital wallet's device.
D. Require public key infrastructure (PKI) to authorize transactions.
Answer: A (LEAVE A REPLY)
Requiring MFA increases the security of digital wallets by adding an additional layer of authentication, making it harder for unauthorized users to gain access. This aligns withAccess Control Standardsand significantly reduces the likelihood of fraud.

NEW QUESTION: 564
Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?
A. Deleting the data from the file system
B. Cryptographically scrambling the data
C. Formatting the cloud storage at the block level
D. Degaussing the cloud storage media
Answer: (SHOW ANSWER)
The best way to ensure data is properly sanitized while in cloud storage is to cryptographically scramble the data. Cryptographic scrambling is the process of transforming data into an unreadable form using a secret key or algorithm. Cryptographic scrambling protects the data from unauthorized access, modification, or deletion, even if the cloud storage provider or a third party gains access to the data. Cryptographic scrambling also ensures that the data can be restored to its original form using the same key or algorithm, if needed. The other options are not as effective as cryptographic scrambling, because they either do not completely remove the data, or they make it impossible to recover the data. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.3.1, page 3-21.

NEW QUESTION: 565
A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?
A. Enable data encryption in the test environment
B. Implement equivalent security in the test environment.
C. Prevent the use of production data for test purposes
D. Mask data before being transferred to the test environment.
Answer: (SHOW ANSWER)
Masking data before being transferred to the test environment is the best recommendation to address the situation where sensitive data from the production environment is required for testing purposes in non-production environments. Data masking is a technique that replaces sensitive data elements with realistic but fictitious data, preserving the format, structure, and meaning of the original data. Data masking ensures that the test data is sufficiently anonymized and de-identified, while still maintaining its functionality and validity for testing purposes. Data masking also reduces the risk of data leakage, exposure, or breach in the test environment, which may have lower security controls than the production environment. The other options are not the best recommendations, as they do not adequately protect the sensitive data or meet the testingrequirements. Enabling data encryption in the test environment may protect the data from

unauthorized access, but it does not prevent the data from being decrypted by authorized users who may misuse or mishandle it. Implementing equivalent security in the test environment may be costly, complex, or impractical, and it may not be feasible to replicate the same level of security controls as in the production environment. Preventing the use of production data for test purposes may not be possible or desirable, as production data may be required to ensure the accuracy, reliability, and quality of the testing results. References = P = NP: Cloud dataprotection in vulnerable non-production environments ...; Data masking secures sensitive data in non-production environments ...; CRISC EXAM TOPIC 2 LONG Flashcards | Quizlet

NEW QUESTION: 566
Which of the following would BEST ensure that identified risk scenarios are addressed?
A. Reviewing the implementation of the risk response
B. Creating a separate risk register for key business units
C. Performing real-time monitoring of threats
D. Performing regular risk control self-assessments
Answer: (SHOW ANSWER)
The best way to ensure that identified risk scenarios are addressed is to review the implementation of the risk response. The risk response is the action or plan that is taken to reduce, avoid, transfer, or accept the risk, depending on the chosen risk treatment option1. Reviewing the implementation of the risk response means checking whether the risk response actions are executed as planned, whether they are effective and efficient in mitigating the risk, and whether they are aligned with the organization's objectives and risk appetite2.
Reviewing the implementation of the risk response helps to monitor and control the risk, identify any gaps or issues, and make any necessary adjustments or improvements. The other options are not the best ways to ensure that identified risk scenarios are addressed, as they are either less comprehensive or less specific than reviewing the implementation of the risk response. Creating a separate risk register for key business units is a way of documenting and tracking the risks that affect different parts of the organization. However, this is not the same as addressing the risk scenarios, as it does not indicate how the risks are treated or resolved.
Performing real-time monitoring of threats is a way of detecting and responding to any changes or events that may increase the likelihood or impact of the risks. However, this is not the same as addressing theriskscenarios, as it does not measure the effectiveness or efficiency of the risk response actions.
Performing regular risk control self-assessments is a way of evaluating and testing the design and operation of the controls that are implemented to mitigate the risks. However, this is not the same as addressing the risk scenarios, as it does not cover the other aspects of the risk response, such as risk avoidance, transfer, or acceptance. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.7, Page 59.

NEW QUESTION: 567
Which of the following functions can be performed by any of the three lines of defense?
A. Monitoring control effectiveness

B. Operating control activities
C. Designing control functions
D. Assuring control processes
Answer: (SHOW ANSWER)
Monitoring control effectivenesscan be done by all lines to varying degrees. The first line monitors during execution, the second provides oversight, and the third provides independent assurance.
Reference:CRISC Manual - Domain 1, Slide 44-47

NEW QUESTION: 568
The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?
A. Insufficient risk tolerance
B. Optimized control management
C. Effective risk management
D. Over-controlled environment
Answer: (SHOW ANSWER)
The situation where the cost of maintaining a control has grown to exceed the potential loss is best described as an over-controlled environment, as it indicates that the control is not cost-effective and may be unnecessary or excessive. Insufficient risk tolerance, optimized control management, and effective risk management are not the best descriptions, as they do not reflect the imbalance between the control cost and the potential loss. References = CRISC Review Manual, 7th Edition, page 149.

NEW QUESTION: 569
The PRIMARY basis for selecting a security control is:
A. to achieve the desired level of maturity.
B. the materiality of the risk.
C. the ability to mitigate risk.
D. the cost of the control.
Answer: (SHOW ANSWER)
The PRIMARY basis for selecting a security control is the ability to mitigate risk, because it is the measure of how well the control can prevent or reduce the occurrence or impact of the risk, and how effectively the control can achieve the desired level of security and protection for the system and the data. The ability to mitigate risk is the most important criterion for selecting a security control, as it directly relates to the purpose and value of the control. The other options are not the primary basis, because:
Option A: To achieve the desired level of maturity is a goal of selecting a security control, but not the primary basis. The desired level of maturity is the state or condition of the security control that reflects its quality, consistency, and reliability, and it should be aligned with the organization's security objectives and standards. The desired level of maturity is a result of selecting a security control, not a reason for selecting it.
Option B: The materiality of the risk is a factor of selecting a security control, but not the primary basis. The materiality of the risk is the degree or extent of the risk that affects the organization's performance, reputation, and value, and it should be considered when selecting a security control, but it is not the only or

the most important factor. The materiality of the risk is an input to selecting a security control, not an output of selecting it.
Option D: The cost of the control is a constraint of selecting a security control, but not the primary basis. The cost of the control is the amount of resources and expenditure that are required to implement and maintain the control, and it should be balanced with the benefit and effectiveness ofthe control, but it is not the only or the most important constraint. The cost of the control is a limitation of selecting a security control, not a motivation for selecting it. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 211.

NEW QUESTION: 570

Which of the following BEST indicates the effectiveness of anti-malware software?

A. Number of staff hours lost due to malware attacks
B. Number of downtime hours in business critical servers
C. Number of patches made to anti-malware software
D. Number of successful attacks by malicious software
Answer: (SHOW ANSWER)
The effectiveness of anti-malware software is the degree to which it can detect, prevent, and remove malicious software (malware) from the system or network. Malware is any software that is designed to harm, exploit, or compromise the functionality, security, or privacy of the system or network1. Some common types of malware are viruses, worms, Trojans, ransomware, spyware, adware, and rootkits2.
One of the best indicators of the effectiveness of anti-malware software is the number of successful attacks by malicious software, which means the number of times that malware has managed to bypass, evade, or disable the anti-malware software and cause damage or disruption to the system or network. The lower the number of successful attacks, the higher the effectiveness of the anti-malware software. This indicator can measure the ability of the anti-malware software to protect the system or network from known and unknown malware threats, and to respond and recover from malware incidents34.
The other options are not the best indicators of the effectiveness of anti-malware software, because:
Number of staff hours lost due to malware attacks is a measure of the impact or consequence of malware attacks on the productivity or performance of the staff. It does not directly reflect the ability of the anti-malware software to detect, prevent, or remove malware, as there may be other factors that affect the staff hours lost, such as the severity of the attack, the availability of backup or recovery systems, or the skills and awareness of the staff5.
Number of downtime hours in business critical servers is a measure of the impact or consequence of malware attacks on the availability or reliability of the servers. It does notdirectly reflect the ability of the anti-malware software to detect, prevent, or remove malware, as there may be other factors that affect the downtime hours, such as the type of the server, the configuration of the network, or the maintenance of the hardware6.
Number of patches made to anti-malware software is a measure of the maintenance or improvement of the anti-malware software. It does not directly reflect the ability of the anti-malware software to detect, prevent, or remove malware, as there may be other factors that affect the number of patches, such as the frequency of the updates, the quality of the software, or the compatibility of the system7.

References =
What is Malware? - Definition from Techopedia
Common Types of Malware and Their Impact - Techopedia
What is Anti-Malware? Everything You Need to Know (2023) - SoftwareLab
The 10 Best Malware Protection Solutions Compared for 2024 - Techopedia The Cost of Malware Attacks - Security Boulevard The Impact of Malware on Business - Kaspersky What is Patch Management? - Definition from Techopedia

NEW QUESTION: 571
An IT project risk was identified during a monthly steering committee meeting. Which of the following roles is BEST positioned to approve the risk mitigation response?
A. Product owner
B. IT manager
C. Project sponsor
D. Project coordinator
Answer: (SHOW ANSWER)
The project sponsor holds the ultimate accountability for the project's success and is typically responsible for approving significant decisions, including risk mitigation responses. Their role involves ensuring that the project aligns with business objectives and that risks are managed appropriately to achieve desired outcomes.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 1: Governance, Section: Roles and Responsibilities.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 572
Accountability for a particular risk is BEST represented in a:
A. risk register
B. risk catalog
C. risk scenario
D. RACI matrix
Answer: (SHOW ANSWER)
A RACI matrix is a tool that assigns the roles and responsibilities for each risk, such as who is responsible, accountable, consulted, and informed. A RACI matrix helps to clarify the expectations and accountabilities for

each risk owner and stakeholder, and to ensure that the risk is managed and monitored effectively and efficiently.
A risk register is a document that records and tracks the identified risks, their likelihood, impact, and mitigation strategies. A risk register does not assign the accountability for each risk, but rather the ownership and response.
A risk catalog is a collection of risks that have been identified and categorized based on common attributes, such as source, type, or impact. A risk catalog does not assign the accountability for each risk, but rather the classification and description.
A risk scenario is a technique that simulates the possible outcomes of different risk events and assesses their impact on the enterprise's objectives and operations. A risk scenario does not assign the accountability for each risk, but rather the analysis and evaluation.
References: CRISC Certified in Risk and Information Systems Control - Question216; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 216.

NEW QUESTION: 573
Which of the following is MOST important to the integrity of a security log?
A. Least privilege access
B. Inability to edit
C. Ability to overwrite
D. Encryption
Answer: (SHOW ANSWER)
A security log is a record of security-related events or activities that occur in an IT system, network, or application, such as user authentication, access control, firewall activity, or intrusion detection1. Security logscan help to monitor and audit the security posture and performance of the IT environment, and to detect and investigate any security incidents, breaches, or anomalies2.
The integrity of a security log refers to the accuracy and completeness of the log data, and the assurance that the log data has not been modified, deleted, or tampered with by unauthorized or malicious parties3. The integrity of a security log is essential for ensuring the reliability and validity of the log analysis and reporting, and for providing evidence and accountability for security incidents and compliance4.
Among the four options given, the most important factor to the integrity of a security log is the inability to edit. This means that the security log data should be protected from any unauthorized or accidental changes or alterations, such as adding, deleting, or modifying log entries, or changing the log format or timestamps5.
The inability to edit can be achieved by implementing various controls and measures, such as:
Applying digital signatures or hashes to the log data to verify its authenticity and integrity Encrypting the log data to prevent unauthorized access or disclosure Implementing least privilege access to the log data to restrict who can view, modify, or delete the log data Using write-once media or devices to store the log data, such as CD-ROMs or WORM drives Sending the log data to a secure and centralized log server or repository, and using syslog or other protocols to ensure secure and reliable log transmission Performing regular backups and archiving of the log data to prevent data loss or corruption References = Security Log: Best Practices for Logging and Management, Security Audit Logging Guideline, Confidentiality, Integrity, &

Availability: Basics of Information Security, Steps for preserving the integrity of log data, Guide to Computer Security Log Management

NEW QUESTION: 574
Which of the following is the STRONGEST indication an organization has ethics management issues?
A. Employees do not report IT risk issues for fear of consequences.
B. Internal IT auditors report to the chief information security officer (CISO).
C. Employees face sanctions for not signing the organization's acceptable use policy.
D. The organization has only two lines of defense.
Answer: A (LEAVE A REPLY)
According to the CRISC Review Manual, ethics management is the process of ensuring that the enterprise's values and principles are embedded in its culture and practices. Ethics management helps to promote trust, integrity, accountability, and transparency among the stakeholders. One of the key elements of ethics management is to encourage the reporting of IT risk issues and incidents, and to protect the whistleblowers from any retaliation or negative consequences. Therefore, if employees do not report IT risk issues for fear of consequences, it is the strongest indication that the organization has ethics management issues, as it implies that there is a lack of trust, openness, and support in the organization. The other options are not the strongest indications of ethics management issues, as they are related to other aspects of IT governance, such as audit independence, policy compliance, and risk management framework. References = CRISC Review Manual,
7th Edition, Chapter 1, Section 1.3.2, page 34.

NEW QUESTION: 575
Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?
A. Risk appetite is decreased.
B. Inherent risk is increased.
C. Risk tolerance is decreased.
D. Residual risk is increased.
Answer: D (LEAVE A REPLY)
Residual risk is the level of risk that remains after applying controls or other risk treatments. A critical patch is a type of control that aims to reduce the risk of a known vulnerability being exploited by attackers. If the patch implementation fails, the control is ineffective and the risk is not reduced. Therefore, the residual risk is increased, as the organization is still exposed to the potential negative consequences of the vulnerability.
References:
*ISACA, Risk and Information Systems Control Review Manual, 7th Edition, 2020, p. 2111
*ISACA, Practical Patch Management and Mitigation2

NEW QUESTION: 576
An organization has established a policy prohibiting ransom payments if subjected to a ransomware attack. Which of the following is the MOST effective control to support this policy?

A. Conducting periodic vulnerability scanning
B. Creating immutable backups
C. Performing required patching
D. Implementing continuous intrusion detection monitoring
Answer: (SHOW ANSWER)
When an organization has a policy prohibiting ransom payments in the event of a ransomware attack, the most effective control to support this policy is creating immutable backups. Here's why:
* Immutable Backups:
* Definition: Immutable backups are backups that cannot be altered, deleted, or modified in any way once they are created. This ensures that a clean, untampered copy of data is always available.
* Protection Against Ransomware: Ransomware attacks typically encrypt data and demand a ransom to decrypt it. With immutable backups, the organization can restore the affected systems using the backup without paying the ransom, thereby adhering to their policy.
* Effectiveness:
* Restoration Capability: Immutable backups provide a reliable means to restore data to its state before the ransomware attack. This restoration capability negates the need to consider paying the ransom to regain access to encrypted data.
* Compliance with Policy: By having a secure and untouchable backup, the organization ensures compliance with its no-ransom policy as it can recover operations without engaging with the attackers.
* Comparison with Other Options:
* Vulnerability Scanning: While important, this primarily helps in identifying vulnerabilities and does not directly help in data recovery post-ransomware attack.
* Patching: Regular patching reduces the risk of ransomware infection but does not aid in recovery if an attack occurs.
* Intrusion Detection: Continuous monitoring can detect ransomware activities but does not provide a solution for restoring data after an attack.
* References:
* The CRISC Review Manual emphasizes the importance of data backups and specifically highlights the advantages of immutable backups in maintaining data integrity and availability in the face of attacks .

NEW QUESTION: 577
Within the risk management space, which of the following activities could be delegated to a cloud service provider?
A. Control implementation
B. Incident response
C. User access reviews
D. Risk oversight
Answer: (SHOW ANSWER)

NEW QUESTION: 578
Which of the following is MOST important to add to the risk register for a remediated risk scenario?

A. Notification to technical teams of implementation schedules
B. Sign-off by senior executives
C. Evidence of successfully implemented controls
D. Minutes from control design meetings
Answer: C (LEAVE A REPLY)
For closed risks, documented proof that controls are in place and working (e.g., logs, test results) is vital. ISACA's CRISC Manual emphasizes that evidence is required to validate control effectiveness and support audit requirements

NEW QUESTION: 579
Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?
A. Changes in the organization's risk appetite and risk tolerance levels
B. Impact due to changes in external and internal risk factors
C. Changes in residual risk levels against acceptable levels
D. Gaps in best practices and implemented controls across the industry
Answer: (SHOW ANSWER)
The most important information to include when reporting the effectiveness of risk management to senior management is the changes in residual risk levels against acceptable levels, as it indicates how well the risk management process and activities have reduced the risk exposure and impact to the level that is aligned with the risk tolerance and appetite of the organization. The other options are not the most important information, as they are more related to the drivers, factors, or outcomes of risk management, respectively, rather than the effectiveness or value of risk management. References = CRISC Review Manual, 7th Edition, page 109.

NEW QUESTION: 580
The PRIMARY benefit of selecting an appropriate set of key risk indicators (KRIs) is that they:
A. serve as a basis for measuring risk appetite.
B. align with the organization's risk profile.
C. provide a warning of emerging high-risk conditions.
D. provide data for updating the risk register.
Answer: (SHOW ANSWER)
According to the ISACA Risk and Information Systems Control study guide and handbook, the primary benefit of selecting an appropriate set of key risk indicators (KRIs) is that they provide a warning of emerging high-risk conditions. KRIs are metrics that monitor changes in the level of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises, and mitigate them in time. KRIs help risk managers to identify potential threats, assess their impact and likelihood, and take proactive measures to reduce the risk or seize the opportunity12
1: ISACA Risk and Information Systems Control Study Guide, 4th Edition, page 33 2: ISACA Risk and Information Systems Control Handbook, 1st Edition, page 25

NEW QUESTION: 581
Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth"?
A. Average bandwidth usage
B. Peak bandwidth usage
C. Total bandwidth usage
D. Bandwidth used during business hours
Answer: (SHOW ANSWER)
Peak bandwidth usage is the most helpful in defining an early-warning threshold associated with insufficient network bandwidth. Peak bandwidth usage is the maximum amount of data that is transferred over a network connection at a given time. It indicates the highest demand and stress on the network resources and capacity.
By monitoring the peak bandwidth usage, the organization can identify the potential bottlenecks, slowdowns, and disruptions that may occur due to insufficient network bandwidth. The organization can also plan and allocate the network bandwidth accordingly to meet the peak demand and avoid service degradation. The other options are not as helpful as peak bandwidth usage, as they do not reflect the actual or potential network performance issues that may arise due to insufficient network bandwidth. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.3: Key Risk Indicators, page 197.

NEW QUESTION: 582
Which of the following is the MOST effective way to assess the risk associated with outsourcing IT processes?
A. Review the vendor's penetration test results
B. Review the contract and service level agreements (SLAs) periodically
C. Benchmark industry peers using the same vendor services
D. Analyze gaps between the current and future state
Answer: (SHOW ANSWER)
Penetration test resultsprovide direct evidence of the vendor's technical security posture and ability to defend against real-world attacks. This is more effective than reviewing contracts or benchmarking, which are indirect measures.
Reference:CRISC Manual - Domain 2, Slide 174-176

NEW QUESTION: 583
Which type of cloud computing deployment provides the consumer the GREATEST degree of control over the environment?
A. Community cloud
B. Private cloud
C. Hybrid cloud
D. Public cloud
Answer: (SHOW ANSWER)

* A private cloud is a type of cloud computing deployment that provides the consumer exclusive access to a pool of computing resources that are owned, managed, and operated by the consumer or a third-party provider on behalf of the consumer.
* A private cloud provides the consumer the greatest degree of control over the environment, because the consumer can customize and configure the resources according to their specific needs and preferences, and can apply their own security and governance policies and standards.
* The other options are not the types of cloud computing deployment that provide the consumer the greatest degree of control over the environment. They are either shared or limited by the provider's settings and rules.
The references for this answer are:
* Risk IT Framework, page 23
* Information Technology & Security, page 17
* Risk Scenarios Starter Pack, page 15

NEW QUESTION: 584
Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?
A. An increase in the number of risk threshold exceptions
B. An increase in the number of change events pending management review
C. A decrease in the number of key performance indicators (KPIs)
D. A decrease in the number of critical assets covered by risk thresholds
Answer: (SHOW ANSWER)
Risk threshold exceptions are instances when a KRI exceeds or falls below a predefined level or point that triggers an action or a warning. An increase in the number of risk threshold exceptions indicates that the KRIs are not reflecting the current risk exposure or environment accurately or effectively. This may suggest that the KRIs are outdated, irrelevant, or poorly defined. Therefore, the KRIs should be revised to ensure that they are aligned with the organizational objectives, risk appetite, and risk management strategy.
References
*Key Risk Indicators: A Practical Guide | SafetyCulture
*Key Risk Indicators: Examples & Definitions - SolveXia
*Choosing and Using Key Risk Indicators - Institute of Risk Management

NEW QUESTION: 585
Which of the following activities BEST facilitates effective risk management throughout the organization?
A. Reviewing risk-related process documentation
B. Conducting periodic risk assessments
C. Performing a business impact analysis (BIA)
D. Performing frequent audits
Answer: (SHOW ANSWER)
Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating the risks that may affect the achievement of an organization's objectives. The activity that best facilitates effective risk management throughout the organization is conducting periodic risk assessments, which are the systematic and structured methods of identifying and analyzing the potential

sources and consequences of risk events. By conducting periodic risk assessments, an organization can proactively identify and prioritize the risks that pose the greatest threat or opportunity, and implement the appropriate risk responses to optimize the risk exposure and align it with the risk appetite and tolerance. References = CRISC Review Manual, 7th Edition, page 63.

NEW QUESTION: 586

Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

A. Testing in a non-production environment

B. Performing a security control review

C. Reviewing the security audit report

D. Conducting a risk assessment

Answer: (SHOW ANSWER)

Automated information security controls are controls that are implemented or executed by software or hardware, without human intervention, to protect the confidentiality, integrity, and availability of information and systems1. Examples of automated information security controls include firewalls, antivirus software, encryption, authentication, and logging2. The effectiveness of automated information security controls refers to how well they achieve their intended objectives and outcomes, such as preventing, detecting, or responding to security threats or incidents3. The best way to measure the effectiveness of automated information security controls prior to going live is to test them in a non-production environment, which is an environment that simulates the production environment, but does not contain real or sensitive data or systems4. Testing in a non-production environment allows the organization to verify the proper and consistent configuration, functionality, and performance of the automated information security controls, without affecting the normal operations or risking the exposure of the data or systems5. Testing in a non-production environment also enables the organization to identify and resolve any issues or gaps in the automated information security controls, and to evaluate their compatibility and interoperability with other systems or controls6. Performing a security control review, reviewing the security audit report, and conducting a risk assessment are not the best ways to measure the effectiveness of automated information security controls prior to going live, as they do not provide direct and timely information on the configuration, functionality, and performance of the automated information security controls. Performing a security control review is a process that involves checking and verifying that the organization's security controls are up to date, relevant, and effective7. A security control review can help to identify and address any issues or gaps in the security controls, but it does not show the actual behavior and results of the automated information security controls in a realistic environment. Reviewing the security audit report is a process that involves reading and analyzing the findings and recommendations of an independent examination and evaluation of the organization's security controls8.

A security audit report can help to provide assurance and advice on the adequacy and effectiveness of the security controls, but it does not show the current and dynamic status and performance of the automated information security controls in a changing environment. Conducting a risk assessment is a process that involves identifying, analyzing, and evaluating the risks and their potential impacts on the organization's objectives and performance. A risk assessment can help to anticipate and prepare for the risks that may

affect the organization's security, but it does not show the actual impact and outcome of the automated information security controls in a specific scenario. References = 1: Automation Support for Security Control Assessments
- NIST2: Automated Security Control Assessment: When Self-Awareness Matters3: Technology Control Automation: Improving Efficiency, Reducing ... - ISACA4: [What is a Non-Production Environment? | Definition and FAQs] 5: [Why You Need a Non-Production Environment - Plutora] 6: [Testing Automated Security Controls - SANS Institute] 7: A brief guide to assessing risks and controls | ACCA Global8: IT Risk Resources | ISACA : [Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.1: Risk Identification, pp. 57-59.]

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 587
Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?
A. Performing a benchmark analysis and evaluating gaps
B. Conducting risk assessments and implementing controls
C. Communicating components of risk and their acceptable levels
D. Participating in peer reviews and implementing best practices
Answer: (SHOW ANSWER)
A risk-aware culture is a culture that recognizes, understands, and values the importance of risk management in achieving the organization's objectives and goals. A risk-aware culture is also a culture that supports and encourages the identification, assessment, response, and monitoring of risks across the organization, as well as the sharing and learning of risk information and best practices. One of the activities that would best contribute to promoting an organization-wide risk-aware culture is communicating components of risk and their acceptable levels. This is a technique to inform and educate the stakeholders and decision makers about the nature and scope of the risks that the organization faces, as well as the criteria and standards that the organization uses to measure and manage the risks. Communicating components of risk and their acceptable levels can help to increase the awareness and understanding of the risks and their impact on the organization's performance and value, as well as to align the expectations and behaviors of the stakeholders and decision makers with the organization's risk appetite and tolerance. Communicating components of risk and their acceptable levels can also help to foster a transparent and collaborative environment for risk management, where the stakeholders and decision makers can openly discuss and address the risks and their implications, as well as to provide and receive feedback and support. The other options are not the best activities to promote an organization-wide risk-aware culture, although

they may be relevant and useful. Performing a benchmark analysis and evaluating gaps is a technique to compare and improve the organization's risk management process and performance with the industry standards or best practices, as well as to identify and close the gaps or weaknesses in the organization's risk management capabilities or maturity. However, this technique does not necessarily promote a risk-aware culture, as it focuses on the process and performance of risk management, not the attitude and behavior of risk management. Conducting risk assessments and implementing controls is a technique to identify and analyze the risks that the organization faces, as well as to select and execute the appropriate actions to address the risks, such as avoiding, transferring, mitigating, or accepting the risks. However, this technique does not directly promote a risk-aware culture, as it focuses on the actions and outcomes of risk management, not the values and beliefs of risk management. Participating in peer reviews and implementing best practices is a technique to evaluate and enhance the quality and effectiveness of the organization's risk management activities anddeliverables, as well as to adopt and apply the proven and successful methods or solutions for risk management. However, this technique does not effectively promote a risk-aware culture, as it focuses on the improvement and optimization of risk management, not the communication and collaboration of risk management. References = CRISC Review Manual, pages 22-231; CRISC Review Questions, Answers & Explanations Manual, page 982; The 6 keyelements to creating and maintaining a good risk culture3; How to increase risk awareness - Project Management Institute4

NEW QUESTION: 588

Which of the following is the MOST important element of a successful risk awareness training program?

A. Customizing content for the audience

B. Providing incentives to participants

C. Mapping to a recognized standard

D. Providing metrics for measurement

Answer: (SHOW ANSWER)

The most important element of a successful risk awareness training program is customizing content for the audience, because this ensures that the training is relevant, engaging, and effective for the learners. Customizing content for the audience means tailoring the training materials and methods to suit the specific needs, preferences, and characteristics of the target group, such as their roles, responsibilities, knowledge, skills, attitudes, and learning styles. Customizing content for the audience can help to achieve the following benefits:

Increase the motivation and interest of the learners, as they can see the value and applicability of the training to their work and goals.

Enhance the comprehension and retention of the learners, as they can relate the training content to their prior knowledge and experience, and use examples and scenarios that are familiar and realistic to them.

Improve the transfer and application of the learners, as they can practice and apply the training content to their actual work situations and challenges, and receive feedback and support that are relevant and useful to them. References = Implementing risk management training and awareness (part 1) 1

NEW QUESTION: 589

Which of the following is MOST important for a risk practitioner to verify when periodically reviewing risk response action plans?

A. The action plans treat the corresponding risk

B. Budget has been allocated for the action plans

C. Key risk indicators (KRIs) are defined in the action plans

D. The action plans have documented schedules

Answer: (SHOW ANSWER)

NEW QUESTION: 590

Which of the following could indicate a potential weakness in the risk management process of an organization?

Freecram.net

A. Some risk remediation activities from the last assessment are still in progress.

B. The risk scenarios have never been updated.

C. The risk scenario development process was led by an external consultant.

D. The number of risk scenarios is very high.

Answer: (SHOW ANSWER)

Risk scenarios must be regularly reviewed and updated to remain relevant, especially given changing threat landscapes and business processes. A set of scenarios developed five years ago without update is likely outdated and may fail to capture current risks effectively. Ongoing remediation and external involvement are not inherently concerns if properly managed. The number of scenarios depends on scope and is less critical than currency and relevance#5:7, 5:256, 5:168 CRISC_SentenceinNOTE30.pptx#.

NEW QUESTION: 591

Which of the following is MOST important for developing effective key risk indicators (KRIs)?

A. Engaging sponsorship by senior management

B. Utilizing data and resources internal to the organization

C. Including input from risk and business unit management

D. Developing in collaboration with internal audit

Answer: (SHOW ANSWER)

Key risk indicators (KRIs) are metrics used by organizations to monitor and assess potential risks that may impact their objectives and performance. KRIs also provide early warning signals that help organizations identify, analyze, and address risks before they escalate into significant issues1. Effective KRIs are those that are relevant, measurable, predictable, comparable, and informational2. The most important factor for developing effective KRIs is including input from risk and business unit management, as they are the persons who have the best understanding of the risk environment, the risk appetite and tolerance, and the risk factors and impacts of the organization. By including input from risk and business unit management, the organization can ensure that the KRIs are aligned with the organization's strategy, vision, and mission, and that they reflect the current and emerging risks and their potential consequences. Engaging sponsorship by senior management, utilizing data and resources internal to the organization, and developing in collaboration with internal audit are not the most important factors for developing effective KRIs, as they do not provide the same level of insight and relevance as including input from risk and business unit management. Engaging

sponsorship by senior management is a factor that involves obtaining the support and approval of the senior leaders who have the authority and accountability for the organization's performance and governance. Engaging sponsorship by senior management can help to promote the importance and value of KRIs, and to ensure their communication and implementation across the organization, but it does not ensure that the KRIs are appropriate and accurate for the organization's risk profile. Utilizing data and resources internal to the organization is a factor that involves using the information and assets that are available within the organization to support or enable the development of KRIs. Utilizing data and resources internal to the organization can help to enhance the quality and reliability of KRIs, and to reduce the cost and complexity of obtaining external data and resources, but it does not ensure that the KRIs are comprehensive and consistent with the organization's risk environment. Developing in collaboration with internal audit is a factor that involves working with the internal audit function that provides independent and objective assurance and advice on the adequacy and effectiveness of the organization's risk management. Developing in collaboration with internal audit can help to improve the validity and compliance of KRIs, and to provide feedback and recommendations for improvement, but it does not ensure that the KRIs are relevant and realistic for the organization's risk objectives and strategies. References = 1: Key Risk Indicators: A Practical Guide | SafetyCulture2: KRI Framework for Operational Risk Management | Workiva3: [Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.1: Key Risk Indicators, pp. 181-185.]

NEW QUESTION: 592
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?
A. The sum of residual risk levels for each scenario
B. The loss expectancy for aggregated risk scenarios
C. The highest loss expectancy among the risk scenarios
D. The average of anticipated residual risk levels
Answer: (SHOW ANSWER)
Residual risk is the remaining risk after the risk response has been implemented. Residual risk can be expressed as a combination of the probability and impact of the risk scenario, or as a single value such as loss expectancy. Residual risk can be compared with the inherent risk, which is the risk level before considering the existing controls or responses, to evaluate the risk reduction and value creation of the risk response. Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. The best way to provide this information is to calculate the average of anticipated residual risk levels for each risk scenario, and to present it as a single value or a range. This can help to provide a comprehensive and consistent view of the residual risk exposure and performance of the process, as well as to align it with the organization's risk appetite and tolerance. The sum of residual risk levels for each scenario, the loss expectancy for aggregated risk scenarios, or the highest loss expectancy among the risk scenarios are not the best ways to provide the overall residual risk level, as they may overestimate or underestimate the risk exposure and performance of the process, and may not reflect the actual risk reduction and value creation of the risk response. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.2, p. 108-109

NEW QUESTION: 593
A maturity model is MOST useful to an organization when it:
A. benchmarks against other organizations
B. defines a qualitative measure of risk
C. provides a reference for progress
D. provides risk metrics.
Answer: (SHOW ANSWER)
A maturity model is a framework that describes the stages or levels of development and improvement of a certain domain, such as a process, a function, or an organization. A maturity model is most useful to an organization when it provides a reference for progress, meaning that it helps the organization to assess its current state, identify its strengths and weaknesses, set its goals and objectives, and measure itsperformance and improvement over time. A maturity model can also help the organization to compare itself with best practices and standards, but benchmarking against other organizations is not its primary purpose. A maturity model can also help the organization to manage its risks, but defining a qualitative measure of risk or providing risk metrics is not its main function. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.3.2.1, p. 118-119

NEW QUESTION: 594
A risk practitioner is MOST likely to use a SWOT analysis to assist with which risk process?
A. Risk assessment
B. Risk reporting
C. Risk mitigation
D. Risk identification
Answer: (SHOW ANSWER)
SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) is used in the riskidentification phase to comprehensively analyze the organization's internal and externalenvironments. By understanding strengths and weaknesses, internal risks can be identified, while opportunities and threats help to identify external risks.
This method provides a foundation for proactive risk management.

NEW QUESTION: 595
Which of the following risk scenarios should be considered in a disaster recovery plan (DRP)?
A. A vendor failing to notify the organization of a data breach
B. A ransomware attack affecting critical systems
C. Hacking activity leading to theft of sensitive data
D. A pandemic situation requiring remote work
Answer: (SHOW ANSWER)

NEW QUESTION: 596

An organization wants to assess the maturity of its internal control environment. The FIRST step should be to:

A. validate control process execution.

B. determine if controls are effective.

C. identify key process owners.

D. conduct a baseline assessment.

Answer: (SHOW ANSWER)

A baseline assessment is the first step in assessing the maturity of an organization's internal control environment. A baseline assessment is a comprehensive evaluation of the current state of the internal control structure, processes, and activities across the organization. A baseline assessment helps to identify the strengths and weaknesses of the existing internal controls, as well as the gaps and opportunities for improvement. A baseline assessment also provides a reference point for measuring the progress and effectiveness of the internal control improvement initiatives. The other options are not the first steps in assessing the maturity of an internal control environment, although they may be part of the subsequent steps.

Validating control process execution is a technique to verify that the internal control activities are performed as designed and intended. Determining if controls are effective is a process to evaluate the adequacy and efficiency of the internal controls in achieving the desired outcomes and mitigating the risks. Identifying key process owners is a task to assign the roles and responsibilities for the internal control design, implementation, and monitoring to the appropriate individuals or groups within the organization. References = CRISC Review Manual, pages 153-1541; CRISC Review Questions, Answers & Explanations Manual, page 742

NEW QUESTION: 597

A global company s business continuity plan (BCP) requires the transfer of its customer information.... event of a disaster. Which of the following should be the MOST important risk consideration?

A. The difference In the management practices between each company

B. The cloud computing environment is shared with another company

C. The lack of a service level agreement (SLA) in the vendor contract

D. The organizational culture differences between each country

Answer: (SHOW ANSWER)

The most important risk consideration when the global company's business continuity plan (BCP) requires the transfer of its customer information to a cloud computing environment in the event of a disaster is that the cloud computing environment is shared with another company. A cloud computing environment is a service model that provides on-demand access to a shared pool of computing resources, such as servers, storage, networks, and applications. A shared cloud computing environment means that the same computing resources are used by multiple customers or tenants, and that the data and activities of one customer may affect or be affected by the data and activities of another customer. This may pose a significant risk to the security, privacy, and availability of the customer information, as it may be exposed, accessed, modified, or deleted by unauthorized or malicious parties. The other options are not as important as the cloud computing environment being shared with another company, as they are related to the differences, agreements, or

cultures of the company or the country, not the environment or the platform of the customer information transfer. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 598

Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

A. To provide input to the organization's risk appetite

B. To monitor the vendor's control effectiveness

C. To verify the vendor's ongoing financial viability

D. To assess the vendor's risk mitigation plans

Answer: (SHOW ANSWER)

The primary reason to perform periodic vendor risk assessments is to monitor the vendor's control effectiveness. A vendor risk assessment is a process of evaluating the risks associated with outsourcing a service or function to a third-party vendor. The assessment should be performed periodically to ensure that the vendor is complying with the contractual obligations, service level agreements, and security standards, and that the vendor's controls are operating effectively to mitigate the risks. Providing input to the organization's risk appetite, verifying the vendor's ongoing financial viability, and assessing the vendor's risk mitigation plans are other possible reasons, but they are not as important as monitoring the vendor's control effectiveness. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 11; CRISC Review Manual, 6th Edition, page 144.

NEW QUESTION: 599

Because of a potential data breach, an organization has decided to temporarily shut down its online sales order system until sufficient controls can be implemented. Which risk treatment has been selected?

A. Avoidance

B. Acceptance

C. Mitigation

D. Transfer

Answer: (SHOW ANSWER)

Risk avoidance involves ceasing activities that expose the organization to significant risks, such as shutting down the sales order system. This decision aligns with Risk Treatment Strategies aimed at eliminating exposure.

NEW QUESTION: 600

Which of the following practices would be MOST effective in protecting personality identifiable information (Ptl) from unauthorized access in a cloud environment?

Freecram.net

A. Apply data classification policy

B. Utilize encryption with logical access controls

C. Require logical separation of company data

D. Obtain the right to audit

Answer: B (LEAVE A REPLY)

The most effective practice in protecting personally identifiable information (PII) from unauthorized access in a cloud environment is to utilize encryption with logical access controls. Encryption is a technique that transforms the data into an unreadable or unintelligible form, making it inaccessible or unusable by unauthorized parties. Logical access controls are the mechanisms or rules that regulate who can access, view, modify, or delete the data, based on their identity, role, or privilege. By utilizing encryption with logical access controls, the PII can be protected from unauthorized access, disclosure, or theft, both in transit and at rest, in a cloud environment. The other options are not as effective as utilizing encryption with logical access controls, as they are related to the classification, separation, or audit of the data, not the protection or security of the data. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 601

A risk practitioner has been asked to evaluate the adoption of a third-party blockchain integration platform based on the value added by the platform and the organization's risk appetite. Which of the following is the risk practitioner's BEST course of action?

A. Conduct a risk assessment with stakeholders.

B. Conduct third-party resilience tests.

C. Update the risk register with the process changes.

D. Review risk related to standards and regulations.

Answer: (SHOW ANSWER)

Conducting a risk assessment with stakeholders is the best course of action for the risk practitioner to evaluate the adoption of a third-party blockchain integration platform, because it helps to identify, analyze, and evaluate the risks and opportunities associated with the platform, and to compare them with the organization's risk appetite and value proposition. A risk assessment is a process of systematically identifying and assessing the sources and types of risk that an organization faces, and estimating their likelihood and impact. A risk assessment also involves identifying and evaluating the existing or proposed controls or mitigating factors that can reduce or eliminate the risk. A stakeholder is a person or group that has an interest or influence in the organization or its activities, such as customers, employees, shareholders, suppliers, regulators, or partners. A blockchain integration platform is a software solution that enables the organization to connect and interact with blockchain networks or applications, such as cryptocurrencies, smart contracts, or distributed ledgers. A blockchain integration platform can offer benefits such as transparency, security, efficiency, and innovation, but it can also pose risks such as technical complexity, interoperability issues, regulatory uncertainty, or cyberattacks. Therefore, conducting a risk assessment with stakeholders is the best way to evaluate the adoption of a third-party blockchain integration platform, as it helps to understand the benefits and risks of the platform, and to align them with the organization's objectives and risk appetite. Conducting third-party resilience tests, updating the risk register with the process changes, and reviewing risk related to standards and regulations are all important tasks to perform after conducting a risk assessment, but they are not the best course of action, as they depend on the results of the risk assessment. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.2, page 87

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 602
Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?
A. Cost and benefit
B. Security and availability
C. Maintainability and reliability
D. Performance and productivity
Answer: (SHOW ANSWER)
The most important consideration when communicating the risk associated with technology end-of-life to business owners is the cost and benefit of the risk response options. Technology end-of-life is the situation when a technology product or service is no longer supported by the vendor or manufacturer, and may pose security, compatibility, or performance issues. The risk practitioner should communicate the cost and benefit of the possible risk responses, such as replacing, upgrading, or maintaining the technology, to the business owners, and help them to make informed and rational decisions. Security and availability, maintainability and reliability, and performance and productivity are other possible considerations, but they are not as important as the cost and benefit. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 8; CRISC Review Manual, 6th Edition, page 97.

NEW QUESTION: 603
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?
A. Develop a mechanism for monitoring residual risk.
B. Update the risk register with the results.
C. Prepare a business case for the response options.
D. Identify resources for implementing responses.
Answer: (SHOW ANSWER)
The next step for the risk practitioner after identifying risk owners and responses for newly identified risk scenarios is to update the risk register with the results. The risk register is a document that records the details of the risks, such as their sources, causes, consequences, likelihood, impact, and responses. By updating the risk register with the results of the risk workshop, the risk practitioner can ensure that the risk information is current, accurate, and complete, and that the risk owners and responses are clearly defined and communicated.

Developing a mechanism for monitoring residual risk, preparing a business case for the response options, and identifying resources for implementing responses are possible steps that may follow the updating of the risk register, but they are not the next step. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 11; CRISC Review Manual, 6th Edition, page 144.

NEW QUESTION: 604
The MAJOR reason to classify information assets is
A. maintain a current inventory and catalog of information assets
B. determine their sensitivity and critical
C. establish recovery time objectives (RTOs)
D. categorize data into groups
Answer: (SHOW ANSWER)
Information asset classification is the process of assigning a level of sensitivity and criticality to an information asset based on its value, importance, and impact to the organization. The major reason to classify information assets is to determine their sensitivity and criticality, which are the measures of how confidential, proprietary, or sensitive the information is, and how essential, urgent, or time-sensitive the information is for the business operations. By determining the sensitivity and criticality of information assets, the organization can prioritize the protection and recovery of the information assets, implement the appropriate security controls and safeguards, comply with the regulatory and contractual requirements, and manage the information lifecycle and disposal. References = CRISC Review Manual, 7th Edition, page 74.

NEW QUESTION: 605
Which of the following is the result of a realized risk scenario?
A. Technical event
B. Threat event
C. Vulnerability event
D. Loss event
Answer: (SHOW ANSWER)
The result of a realized risk scenario is a loss event. A loss event is an occurrence that causes harm or damage to the organization's assets, resources, or reputation. A loss event is also known as an incident or a breach. A loss event is the outcome of a risk scenario, which is a description of a possible situation or event that could affect the organization's objectives or operations. A risk scenario consists of three elements: a threat, a vulnerability, and an impact. A threat is a potential source of harm or damage. A vulnerability is a weakness or flaw that could be exploited by a threat. An impact is the consequence or effect of a threat exploiting a vulnerability. A risk scenario is realized when a threat exploits a vulnerability and causes an impact, which results in a loss event. The other options are not the result of a realized risk scenario, although they may be part of a risk scenario. A technical event, a threat event, and a vulnerability event are all types of events that could occur in a risk scenario, but they are not the final outcome or result of a risk scenario. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 606
Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?
A. Informed consent
B. Cross border controls
C. Business impact analysis (BIA)
D. Data breach protection
Answer: (SHOW ANSWER)
According to the GDPR, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes1. This means that a business unit can only use personal information for a different purpose if it has obtained the consent of the data subject, or if it has a clear legal basis or obligation to do so2. Therefore, informed consent should be the first consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected.
References = GDPR Article 5 (1) (b) and Article 6 (4)1, ICO Principle (b): Purpose limitation2

NEW QUESTION: 607
Which of the following helps an organization monitor when risk levels exceed acceptable thresholds?
A. Key performance indicators (KPIs)
B. Key risk indicator (KRI) thresholds
C. Risk trends
D. Risk objectives
Answer: (SHOW ANSWER)
A decrease in risk appetite typically results in tighter tolerances and thresholds for KRIs, as the organization becomes less willing to accept certain levels of risk. KPIs and risk objectives may also be impacted but are less directly tied to appetite shifts. Risk trends reflect historical data rather than appetite settings

NEW QUESTION: 608
An organization has contracted with a cloud service provider to support the deployment of a new product. Of the following, who should own the associated risk?
A. The head of enterprise architecture (EA)
B. The IT risk manager
C. The information security manager
D. The product owner
Answer: (SHOW ANSWER)
The product owner should own the associated risk when contracting with a cloud service provider to support the deployment of a new product. The product owner is the person who has the authority and responsibility for defining the product vision, requirements, and priorities. The product owner also has the accountability for the business value and outcomes of the product. Therefore, the product owner should be the one who identifies, assesses, and manages the risks related to the cloud service provider, such as security, compliance, performance, and quality. The product owner should also collaborate with the other

stakeholders, such as the head of EA, the IT risk manager, and the information security manager, to ensure that the cloud service provider meets the organization's standards and expectations. References = Risk and Information Systems Control Study Manual, Chapter 5: IT Risk Mitigation, Section 5.3: IT Risk Mitigation Strategies and Approaches, Page 254; Best Practices to Manage Risks in the Cloud - ISACA.

NEW QUESTION: 609
Which of the following is the BEST method for identifying vulnerabilities?
A. Batch job failure monitoring
B. Periodic network scanning
C. Annual penetration testing
D. Risk assessments
Answer: (SHOW ANSWER)
The best method for identifying vulnerabilities is periodic network scanning. Network scanning is a process of scanning and probing the network devices, systems, and applications to discover and analyze their security weaknesses, such as configuration errors, outdated software, or open ports. Network scanning can help to identify the vulnerabilities that could be exploited by attackers to gain unauthorized access, compromise data, or disrupt services. Periodic network scanning is the best method, because it can provide a regular and comprehensive view of the network security posture, and it can detect and address the new or emerging vulnerabilities in a timely manner. Periodic network scanning can also help to comply with the legal and regulatory requirements and standards for network security, such as the ISO/IEC 27001, the NIST SP 800-53, or the PCI DSS123. The other options are not the best method, although they may be useful or complementary to periodic network scanning. Batch job failure monitoring is a process of monitoring and reporting the failures or errors that occur during the execution of batch jobs, such as data processing, backup, or synchronization. Batch job failure monitoring can help to identify the operational or technical issues that affect the performance or availability of the network services, but it does not directly identify the security vulnerabilities or the potential threats. Annual penetration testing is a process of simulating a real-world attack on the network devices, systems, and applications to evaluate their security defenses and resilience.
Penetration testing can help to identify and exploit the vulnerabilities that could be used by attackers to compromise the network security, and to provide recommendations for improvement. However, annual penetration testing is not the best method, because it is not frequent or consistent enough to keep up with the changing and evolving network security landscape, and it may not cover all the network components or scenarios. Risk assessments are a process of identifying, analyzing, and evaluating the risks associated with the network devices, systems, and applications. Risk assessments can help to estimate the probability and impact of the vulnerabilities and the threats, and to prioritize and respond to the risks accordingly. However, risk assessments are not the same as or a substitute for vulnerability identification, as they rely on the vulnerability information as an input, rather than an output. References = Vulnerability Testing: Methods, Tools, and 10 Best Practices, ISO/IEC 27001 Information Security Management, NIST SP 800-53 Rev. 5

NEW QUESTION: 610
Which of the following will BEST help to improve an organization's risk culture?

A. Maintaining a documented risk register
B. Establishing a risk awareness program
C. Rewarding employees for reporting security incidents
D. Allocating resources for risk remediation
Answer: (SHOW ANSWER)
A risk awareness program is a set of activities that aim to educate and inform employees about the organization's risk culture, policies, and procedures. A risk awareness program can help improve an organization's risk culture by enhancing the employees' understanding of risk, their roles and responsibilities in risk management, and the benefits of risk mitigation. A risk awareness program can also foster a culture of openness, trust, and collaboration among employees, managers, and stakeholders, which can improve the organization's risk performance and resilience.
Maintaining a documented risk register, rewarding employees for reporting security incidents, and allocating resources for risk remediation are also important aspects of risk management, but they do not directly address the organization's risk culture, which is the shared values, beliefs, and attitudes that influence how risk is perceived and handled within the organization.

NEW QUESTION: 611
The PRIMARY advantage of involving end users in continuity planning is that they:
A. have a better understanding of specific business needs
B. can balance the overall technical and business concerns
C. can see the overall impact to the business
D. are more objective than information security management.
Answer: (SHOW ANSWER)
Continuity planning is the process of developing strategies and plans to ensure the continuity of critical business functions and processes in the event of a disruption or disaster. Continuity planning involves identifying the risks, impacts, and recovery options for various scenarios, as well as testing and updating the plans regularly. The primary advantage of involving end users in continuity planning is that they have a better understanding of specific business needs, such as the operational requirements, the customer expectations, and the dependencies and interdependencies of the business processes. End users can provide valuable input and feedback on the continuity plans, as well as participate in the testing and validation of the plans. End users can also help to ensure the alignment of the continuity plans with the business objectives and priorities, as well as the compliance with the relevant standards and regulations. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.4.1, p. 204-205

NEW QUESTION: 612
During the creation of an organization's IT risk management program, the BEST time to identify key risk indicators (KRIs) is while:
A. Interviewing data owners
B. Reviewing risk response plans with internal audit
C. Developing a risk monitoring process
D. Reviewing an external risk assessment

Answer: (SHOW ANSWER)
KRIs should be identified during the development of a risk monitoring process to ensure alignment with organizational objectives and effective risk tracking. This reflectsProactive Risk Monitoring.

NEW QUESTION: 613
Which of the following is the MOST important responsibility of a risk owner?
A. Testing control design
B. Accepting residual risk
C. Establishing business information criteria
D. Establishing the risk register
Answer: (SHOW ANSWER)
Accepting residual risk is the most important responsibility of a risk owner, as it implies that the risk owner is accountable for the risk and its impact on the enterprise's objectives and operations. Residual risk is the risk that remains after the implementation of controls, and it should be aligned with the risk appetite and tolerance of the enterprise. The risk owner is responsible for implementing the risk response strategies and monitoring the risk status and outcomes, as well as for reporting and escalating the risk issues and incidents. Testing control design, establishing business information criteria, and establishing the risk register are not the most important responsibilities of a risk owner, but rather the tasks or activities that the risk owner may perform or delegate as part of the risk management process. References = CRISC Certified in Risk and Information Systems Control - Question218; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 218.

NEW QUESTION: 614
Which of the following would present the GREATEST challenge for a risk practitioner during a merger of two organizations?
A. Variances between organizational risk appetites
B. Different taxonomies to categorize risk scenarios
C. Disparate platforms for governance, risk, and compliance (GRC) systems
D. Dissimilar organizational risk acceptance protocols
Answer: (SHOW ANSWER)
The greatest challenge for a risk practitioner during a merger of two organizations is the variances between organizational risk appetites, as they may indicate a significant difference in the risk culture, strategy, and objectives of the two organizations, and may require a complex and lengthy process of alignment and integration. Different taxonomies to categorize risk scenarios, disparate platforms for governance, risk, and compliance (GRC) systems, and dissimilar organizational risk acceptance protocols are not the greatest challenges, as they are more related to the technical, operational, or procedural aspects of risk management, rather than the strategic or cultural aspects of risk management. References = CRISC Review Manual, 7th Edition, page 109.

NEW QUESTION: 615

An organization that has been the subject of multiple social engineering attacks is developing a risk awareness program. The PRIMARY goal of this program should be to:

A. reduce the risk to an acceptable level.

B. communicate the consequences for violations.

C. implement industry best practices.

D. reduce the organization's risk appetite

Answer: (SHOW ANSWER)

According to the CRISC Review Manual (Digital Version), the primary goal of a risk awareness program is to reduce the risk to an acceptable level by increasing the knowledge and understanding of the risk among the stakeholders. A risk awareness program should:

Educate the stakeholders about the sources, types and impacts of IT-related risks Explain the roles and responsibilities of the stakeholders in the risk management process Promote a risk-aware culture that supports the risk appetite and risk tolerance of the organization Provide guidance and tools for identifying, assessing, responding and monitoring IT-related risks Encourage the reporting and escalation of risk issues and incidents Reinforce the benefits and value of effective risk management References = CRISC Review Manual (Digital Version), Chapter 4: IT Risk Monitoring and Reporting, Section 4.2: IT Risk Reporting, pp. 224-2251

NEW QUESTION: 616

A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which ot the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.

B. Document the gap in the risk register and report to senior management.

C. Include a right to audit clause in the service provider contract.

D. Advise the risk owner to accept the risk.

Answer: (SHOW ANSWER)

The best course of action for the risk practitioner who has identified that the agreed RTO with a SaaS provider is longer than the business expectation is to collaborate with the risk owner to determine the risk response plan. The risk owner is the person who has the authority and accountability to manage the risk within their scope of responsibility. The risk response plan is the document that describes the actions and resources needed to address the risk. By collaborating with the risk owner, the risk practitioner can help to analyze the gap between the agreed RTO and the business expectation, evaluate the potential impact and consequences, and select the most appropriate risk response option, such as avoiding, reducing, transferring, or accepting the risk. Documenting the gap in the risk register, including a right to audit clause in the service provider contract, or advising the risk owner to accept the risk are not the best courses of action, because they do not address the root cause of the problem, or provide a solution to reduce the risk to an acceptable level. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.1, page 4-23.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 617
As part of an overall IT risk management plan, an IT risk register BEST helps management:
A. align IT processes with business objectives.
B. communicate the enterprise risk management policy.
C. stay current with existing control status.
D. understand the organizational risk profile.
Answer: (SHOW ANSWER)
An IT risk register is a document that is used as a risk management tool to identify, analyze, and track the potential risks related to the use of information technology within an organization. An IT risk register helps management to understand the organizational risk profile, which is a comprehensive and structured representation of the risks that the organization faces. The risk profile helps the organization to understand its risk exposure, appetite, and tolerance, and to align its risk management strategy with its business objectives and context. The risk register is an essential input for creating and updating the risk profile, as it provides the data and analysis of the risks that need to be prioritized and addressed12. The other options are not the best answers, as they are either not directly shown or derived from the IT risk register. Aligning IT processes with business objectives is a goal of IT governance, which may be influenced by the IT risk register, but not solely determined by it. Communicating the enterprise risk management policy is a responsibility of the senior management and the board of directors, which may use the IT risk register as a reference, but not as the main source. Staying current with existing control status is a function of IT audit and assurance, which may rely on the IT risk register as a basis, but not as the only evidence. References = Risk Register: A Project Manager's Guide with Examples [2023] * Asana; Complete Guide to IT Risk Management | CompTIA

NEW QUESTION: 618
Which of the following represents a vulnerability?
A. An identity thief seeking to acquire personal financial data from an organization
B. Media recognition of an organization's market leadership in its industry
C. A standard procedure for applying software patches two weeks after release
D. An employee recently fired for insubordination
Answer: (SHOW ANSWER)
A vulnerability is a weakness or gap in a system, application, or network that can be exploited by a threat to cause harm or gain unauthorized access1. A vulnerability can be caused by various factors, such as design flaws, coding errors, configuration errors, or outdated software2.

Among the four options given, only option C (a standard procedure for applying software patches two weeks after release) represents a vulnerability. This is because software patches are updates or fixes that address security weaknesses or bugs in software applications or systems3. By applying software patches two weeks after release, the organization is exposing itself to the risk of being attacked or compromised by malicious actors who may exploit the known vulnerabilities in the software before they are patched. This risk is especially high if the software is internet-facing or critical to the organization's operations4.
References = What is a Vulnerability?, Vulnerability Definition & Meaning - Merriam-Webster, Vulnerability Patching: A Resource Guide - Rezilion, Why is Software Vulnerability Patching Crucial for Your Software and ...

NEW QUESTION: 619
Which of the following is the PRIMARY purpose of a risk register?
A. It aligns risk scenarios to business objectives.
B. It guides management in determining risk appetite.
C. It monitors the performance of risk and control owners.
D. It provides management with a risk inventory.
Answer: (SHOW ANSWER)

NEW QUESTION: 620
During a post-implementation review for a new system, users voiced concerns about missing functionality.
Freecram.net
Which of the following is the BEST way for the organization to avoid this situation in the future?
A. Test system reliability and performance.
B. Adopt an Agile development approach.
C. Conduct user acceptance testing (UAT).
D. Adopt a phased changeover approach.
Answer: (SHOW ANSWER)
Conducting User Acceptance Testing (UAT) is the best way for an organization to avoid situations where users voice concerns about missing functionality after a system implementation.
User Acceptance Testing (UAT):
Definition:UAT involves testing the system with actual users to ensure it meets their needs and requirements. It verifies that the system performs in real-world scenarios as expected by the users.
Involvement of Users:UAT includes the end-users in the testing process, ensuring that their feedback is incorporated and that the system functionalities align with their expectations.
Benefits:
Identifying Gaps:UAT helps in identifying gaps between the delivered system and user expectations. This early detection allows for adjustments before the system goes live.
Improved Satisfaction:By involving users in the testing process, the likelihood of the system meeting their needs increases, leading to higher user satisfaction and reduced post-implementation issues.
References:

The CRISC Review Manual and best practices in project management emphasize the importance of UAT in ensuring that the system meets user requirements and avoids post-implementation functionality concerns .

NEW QUESTION: 621
Which of the following BEST protects organizational data within a production cloud environment?
A. Data encryption
B. Continuous log monitoring
C. Right to audit
D. Data obfuscation
Answer: (SHOW ANSWER)
Data encryption is the best method to protect organizational data within a production cloud environment, as it ensures the confidentiality, integrity, and availability of the data. Data encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt the data. Data encryption can protect data at rest (stored in the cloud) and data in transit (transferred over the network) from unauthorized access, modification, or deletion by malicious actors or accidental errors. Data encryption can also help organizations comply with legal, regulatory, and contractual requirements for data protection and privacy, such as GDPR, CCPA, and PCI DSS.
References:
*The Complexity Conundrum: Simplifying Data Security1
*Practical Data Security and Privacy for GDPR and CCPA2

NEW QUESTION: 622
A risk practitioner identifies an increasing trend of employees copying company information unrelated to their job functions to USB drives. Which of the following elements of the risk register should be updated to reflect this observation?
A. Risk impact
B. Key risk indicator (KRI)
C. Risk appetite
D. Risk likelihood
Answer: (SHOW ANSWER)
When a risk practitioner identifies an increasing trend of employees copying company information unrelated to their job functions to USB drives, the element of the risk register that should be updated is the risk likelihood. Here's why:
* Risk Likelihood:
* Risk likelihood refers to the probability that a risk event will occur.
* Observing an increasing trend of inappropriate behavior (such as copying sensitive information) indicates a higher probability of occurrence, thus increasing the risk likelihood.
* Risk Impact:
* While the impact of such actions could be significant, the increasing trend specifically affects the likelihood rather than the immediate impact.
* The risk impact remains constant unless there is a change in the potential damage caused by the action.

* Key Risk Indicator (KRI):
* This observation might serve as a KRI, but the immediate action is to update the likelihood in the risk register, reflecting the increased probability.
* Risk Appetite:
* Risk appetite defines the level of risk an organization is willing to accept. This observation suggests a deviation but does not directly affect the risk appetite itself.
* References:
* The CRISC Review Manual emphasizes the importance of regularly updating the risk likelihood based on new observations and trends (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.9.1 Inherent Risk).

NEW QUESTION: 623
An organization recently implemented new technologies that enable the use of robotic process automation. Which of the following is MOST important to reassess?
A. Risk profile
B. Risk tolerance
C. Risk capacity
D. Risk appetite
Answer: (SHOW ANSWER)
The risk profile is the most important thing to reassess when an organization implements new technologies that enable the use of robotic process automation (RPA). The risk profile is a comprehensive and dynamic view of the organization's risks, their ratings, responses, and status. RPA can introduce new risks or change the existing risks related to the organization's objectives, operations, and performance. For example, RPA can create risks such as system failures, data breaches, compliance violations, human errors, or ethical dilemmas.
Therefore, the organization should reassess its risk profile to identify, assess, treat, monitor, and review the risks associated with RPA, and to ensure that the risk management strategy is aligned with the business needs and expectations.
References:
*ISACA, Robotic Process Automation for Internal Audit1
*ISACA, Key Considerations for Robotic Process Automation2

NEW QUESTION: 624
Sensitive data has been lost after an employee inadvertently removed a file from the premises, in violation of organizational policy. Which of the following controls MOST likely failed?
A. Background checks
B. Awareness training
C. User access
D. Policy management
Answer: (SHOW ANSWER)

Awareness training is the most likely control that failed in this scenario, as it is designed to educate employees on the proper handling and protection of sensitive data, and the consequences of violating the organizational policy. Awareness training can help to prevent or reduce the occurrence of human errors, such as inadvertently removing a file from the premises, that may result in data loss or breach. The other options are not the most likely controls that failed, as they are either not directly related to the scenario or not sufficient to prevent the incident. Background checks are used to verify the identity, qualifications, and trustworthiness of potential or current employees, but they do not ensure that employees will always follow the policy or avoid mistakes. User access is used to restrict the access to information systems or resources based on the identity, role, or credentials of the user, but it does not prevent the user from copying or removing the data once they have access. Policy management is used to create, communicate, and enforce the organizational policy, but it does not ensure that employees will understand or comply with the policy. References = Sensitive Data Essentials - The Lifecycle Of A Sensitive File; Personal data breach examples | ICO; How do I prevent staff accidentally sending personal information ... - GCIT; 10 Ways to Protect Sensitive Employee Information; My personal data has been lost after a breach, what are my rights ...

NEW QUESTION: 625
Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?
A. Independent audit report
B. Control self-assessment
C. MOST important to update when an
D. Service level agreements (SLAs)
Answer: (SHOW ANSWER)
The MOST important thing to review when determining whether a potential IT service provider's control environment is effective is an independent audit report, because it provides an objective and reliable assessment of the service provider's controls and compliance with standards and regulations. The other options are not as important as an independent audit report, because:
Option B: Control self-assessment is a subjective and voluntary process that may not reflect the actual effectiveness of the service provider's controls.
Option C: This option is incomplete and irrelevant to the question.
Option D: Service level agreements (SLAs) are contractual agreements that specify the expected performance and availability of the service provider, but they do not necessarily indicate the effectiveness of the service provider's controls. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA,
2020, p. 195.

NEW QUESTION: 626
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an anti-virus program?
A. Frequency of anti-virus software updates
B. Number of alerts generated by the anti-virus software

C. Number of false positives detected over a period of time
D. Percentage of IT assets with current malware definitions
Answer: (SHOW ANSWER)
An anti-virus program is a software that detects and removes malicious software, such as viruses, worms, or ransomware, from the IT assets, such as computers, servers, or networks. The effectiveness of an anti-virus program can be measured by the key performance indicators (KPIs) that reflect the achievement of the program objectives and the alignment with the enterprise's risk appetite and tolerance. The best KPI to measure the effectiveness of an anti-virus program is the percentage of IT assets with current malware definitions. Malware definitions are the files or databases that contain the signatures or patterns of the known malicious software, and they are used by the anti-virus program to scan and identify the malware. The percentage of IT assets with current malware definitions indicates how well the anti-virus program is able to protect the IT assets from the latest or emerging threats, and reduce the exposure and impact of the risks associated with the malware. The other options are not as good as the percentage of IT assets with current malware definitions, as they may not reflect the quality or timeliness of the protection, or the alignment with the enterprise's risk appetite and tolerance. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.3.2.1, pp. 171-172.

NEW QUESTION: 627
Which of the following is the GREATEST risk associated with the misclassification of data?
A. inadequate resource allocation
B. Data disruption
C. Unauthorized access
D. Inadequate retention schedules
Answer: C (LEAVE A REPLY)
According to the CRISC Review Manual, the greatest risk associated with the misclassification of data is unauthorized access, because it can result in the loss of confidentiality, integrity, and availability of the data. Data classification is the process of assigning categories to data based on its sensitivity and value to the organization. Data classification helps to determine the appropriate level of protection and handling for the data. If the data is misclassified, it may not receive the adequate level of security controls, and it may be accessed by unauthorized or inappropriate users. The other options are not the greatest risks associated with the misclassification of data, as they are less likely or less severe than unauthorized access. Inadequate resource allocation is the risk of not allocating sufficient resources to protect the data, which may affect its availability and performance. Data disruption is the risk of losing or corrupting the data, which may affect its integrity and availability. Inadequate retention schedules is the risk of not retaining the data for the required period of time, which may affect its compliance and usability. References = CRISC Review Manual, 7th Edition, Chapter 4, Section 4.1.1, page 161.

NEW QUESTION: 628
A failed IT system upgrade project has resulted in the corruption of an organization's asset inventory database.
Which of the following controls BEST mitigates the impact of this incident?

A. Encryption
B. Authentication
C. Configuration
D. Backups
Answer: (SHOW ANSWER)
Backups are the best control to mitigate the impact of a failed IT system upgrade project that has resulted in the corruption of an organization's asset inventory database, as they allow the organization to restore the data from a previous state and resume normal operations. Encryption, authentication, and configuration are not the best controls, as they do not address the data corruption issue, but rather the data security, access, and quality issues, respectively. References = CRISC Review Manual, 7th Edition, page 153.

NEW QUESTION: 629
Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?
A. Device corruption
B. Data loss
C. Malicious users
D. User support
Answer: (SHOW ANSWER)
A bring your own device (BYOD) initiative allows employees to use their personal devices, such as smartphones, tablets, or laptops, for work purposes. This can provide benefits such as increased productivity, flexibility, and employee satisfaction. However, it also introduces significant risks, such as data loss, data leakage, malware infection, unauthorized access, and compliance violations. Among these risks, data loss is of greatest concern for an organization, as it can have severe consequences, such as reputational damage, legal liability, financial loss, and competitive disadvantage. Data loss can occur due to various reasons, such as device theft, loss, damage, or disposal, accidental deletion, unauthorized transfer, or malicious attack.
Therefore, an organization considering the adoption of a BYOD initiative should implement appropriate controls, such as encryption, authentication, remote wipe, backup, and data classification, to protect the data stored or accessed on the personal devices. References = Bring Your Own Device (BYOD) Policy: What You Need to Know, BYOD Risks: What You Need to Know, BYOD Security: 8 Risks and How to Mitigate Them

NEW QUESTION: 630
Which of the following helps ensure compliance with a nonrepudiation policy requirement for electronic transactions?
Freecram.net
A. Digital signatures
B. Encrypted passwords
C. One-time passwords
D. Digital certificates
Answer: (SHOW ANSWER)

Nonrepudiation is the ability to prevent or deny the parties involved in an electronic transaction from disputing or rejecting the validity or authenticity of the transaction. Nonrepudiation ensures that the parties cannot claim that they did not send or receive the transaction, or that the transaction was altered or tampered with.
The tool that helps ensure compliance with a nonrepudiation policy requirement for electronic transactions is digital signatures, which are the electronic equivalents of handwritten signatures that are used to verify the identity and integrity of the sender and the content of the transaction. Digital signatures are generated by applying a cryptographic algorithm to the transaction, using the sender's private key, which is a secret and unique code that only the sender knows and possesses. The digital signature can be verified by the receiver or any third party, using the sender's public key, which is a code that is publicly available and corresponds to the sender's private key. The digital signature can prove that the transaction was sent by the sender, and that the transaction was not altered or tampered with during the transmission.
The other options are not the tools that help ensure compliance with a nonrepudiation policy requirement for electronic transactions, because they do not provide the same level of verification and validation that digital signatures provide, and they may not be sufficient or effective to prevent or deny the parties from disputing or rejecting the transaction.
Encrypted passwords are the passwords that are converted into a secret or unreadable form, using a cryptographic algorithm, to protect them from unauthorized access or disclosure. Encrypted passwords can help to ensure the confidentiality and security of the passwords, but they are not the tools that help ensure compliance with a nonrepudiation policy requirement for electronic transactions, because they do not verify the identity and integrity of the sender and the content of the transaction, and they may not prevent or deny the parties from disputing or rejecting the transaction.
One-time passwords are the passwords that are valid or usable for only one session or transaction, and that are randomly generated or derived from a dynamic factor, such as time, location, or device. One-time passwords can help to enhance the security and authentication of the parties involved in the transaction, but they are not the tools that help ensure compliance with a nonrepudiation policy requirement for electronic transactions, because they do not verify the identity and integrity of the sender and the content of the transaction, and they may not prevent or deny the parties from disputing or rejecting the transaction.
Digital certificates are the electronic documents that contain the information and credentials of the parties involved in the transaction, such as their name, public key, expirationdate, etc., and that are issued and signed by a trusted authority or entity, such as a certificate authority or a digital signature provider. Digital certificates can help to establish and confirm the identity and trustworthiness of the parties involved in the transaction, but they are not the tools that help ensure compliance with a nonrepudiation policy requirement for electronic transactions, because they do not verify the identity and integrity of the sender and the content of the transaction, and they may not prevent or deny the parties from disputing or rejecting the transaction.
References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 40-41, 47-48, 54-55, 58-59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 197 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 631
Which of the following risk register updates is MOST important for senior management to review?
A. Extending the date of a future action plan by two months

B. Retiring a risk scenario no longer used
C. Avoiding a risk that was previously accepted
D. Changing a risk owner
Answer: (SHOW ANSWER)
A risk register is a document that records and tracks the information and status of the identified risks and their responses. It includes the risk description, category, source, cause, impact, probability, priority, response, owner, action plan, status, etc.
A risk register update is a change or modification to the information or status of the risks and their responses in the risk register. It may be triggered by the occurrence or resolution of a risk event, the identification or evaluation of a new or emerging risk, the implementation or completion of a risk response, the monitoring or review of the risk performance, etc.
The most important risk register update for senior management to review is avoiding a risk that was previously accepted, which means that the organization has decided to eliminate or withdraw from the risk exposure or activity that may cause the risk, instead of tolerating or retaining the risk as before. This may indicate a significant change in the organization's risk appetite, strategy, objectives, or environment, and it may have a major impact on the organization's performance and value.
The other options are not the most important risk register updates for senior management to review, because they do not indicate a significant change or impact on the organization's risk profile or performance.
Extending the date of a future action plan by two months means that the organization has postponed the implementation or completion of the planned actions or measures to address the risk, due to some reasons or constraints. This may indicate a delay or deviation from the expected or desired risk outcome, but it may not have a major impact on the organization's performance and value, unless the risk is very urgent or critical.
Retiring a risk scenario no longer used means that the organization has removed or discarded the risk scenario that is no longer relevant or applicable to the organization's objectives or operations, due to some changes or developments. This may indicate a reduction or improvement in the organization's risk exposure or level, but it may not have a major impact on the organization's performance and value, unless the risk scenario was very significant or influential.
Changing a risk owner means that the organization has assigned or transferred the responsibility and accountability for the risk and its response to a different person or role, due to some reasons or circumstances.
This may indicate a change or improvement in the organization's risk governance or culture, but it may not have a major impact on the organization's performance and value, unless the risk owner was very ineffective or inappropriate. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-
59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 160 CRISC Practice Quiz and Exam Prep

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 632
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?
A. Migrate all data to another compliant service provider.
B. Analyze the impact of the provider's control weaknesses to the business.
C. Conduct a follow-up audit to verify the provider's control weaknesses.
D. Review the contract to determine if penalties should be levied against the provider.
Answer: (SHOW ANSWER)
An independent security audit report is a document that provides an objective and comprehensive assessment of the security posture and practices of a cloud service provider (CSP), based on a set of standards, criteria, or frameworks1. An independent security audit report can help an organization to evaluate the risks and benefits of using a CSP, and to ensure that the CSP meets the organization's security and compliance requirements2.
If an organization receives an independent security audit report of its CSP that indicates significant control weaknesses, the next step that should be done in response to this report is to analyze the impact of the provider's control weaknesses to the business. This means that the organization should:
Identify and prioritize the business processes, functions, or objectives that depend on or are affected by the CSP's services Assess the potential consequences and likelihood of the control weaknesses leading to security incidents, breaches, or losses Estimate the financial, operational, reputational, or legal impacts of the security incidents, breaches, or losses Compare the impacts with the organization's risk appetite and tolerance, and determine the level of risk exposure and acceptance Communicate the results of the analysis to the relevant stakeholders and decision-makers3 References = What is a Security Audit?, Cloud Security Audit: A 10-Step Checklist, Independent security audits are essential for cloud service providers. Here's why

NEW QUESTION: 633
What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?
A. Documenting project lessons learned
B. Validating the risk mitigation project has been completed
C. Confirming that the project budget was not exceeded
D. Verifying that the risk level has been lowered
Answer: (SHOW ANSWER)
A post-implementation review (PIR) is a process to evaluate whether the objectives of the project were met and whether the project delivered the expected benefits and outcomes1. The primary objective of a risk

practitioner performing a PIR of an IT risk mitigation project is to verify that the risk level has been lowered as a result of the project implementation2. This can be done by comparing the actual risk level with theexpected risk level, assessing the effectiveness and efficiency of the risk mitigation controls, and identifying any residual or emerging risks3. Documenting project lessons learned, validating the project completion, and confirming the project budget are important aspects of a PIR, but they are not the primary objective for a risk practitioner, as they do not directly measure the impact of the project on the risk level4. References = Risk and Information Systems Control Study Manual, Chapter 5: Risk Response and Mitigation, Section 5.4: Post-Implementation Review, pp. 239-241.

NEW QUESTION: 634
Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?
A. Self-assessments by process owners
B. Mitigation plan progress reports
C. Risk owner attestation
D. Change in the level of residual risk
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after the risk mitigation plans have been implemented. Residual risk reflects the effectiveness of the risk response in reducing the likelihood or impact of the risk. The best evidence that risk mitigation plans have been implemented effectively is the change in the level of residual risk. A change in the level of residual risk can be measured by comparing the risk level before and after the risk mitigation plans have been executed. A change in the level of residual risk can also be evaluated by comparing the actual residual risk with the target or acceptable residual risk. A change in the level of residual risk can demonstrate how well the risk mitigation plans have achieved the risk objectives and met the risk criteria. A change in the level of residual risk can also provide feedback and lessons learned for future risk management activities. References = Residual Risk: Definition, Formula & Management, Residual Risk: What It Is and How to Manage It, Residual Risk: How to Calculate and Manage It.

NEW QUESTION: 635
Which of the following would MOST effectively reduce risk associated with an increased volume of online transactions on a retailer website?
A. Hot backup site
B. Transaction limits
C. Scalable infrastructure
D. Website activity monitoring
Answer: (SHOW ANSWER)
Scalable infrastructure ensures the system can handle increased load without failure, thus minimizing the risk of downtime or degraded performance during traffic spikes.
Reference:CRISC Manual - Domain 3, Slide 327

NEW QUESTION: 636

From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

A. Residual risk is reduced.

B. Staff costs are reduced.

C. Operational costs are reduced.

D. Inherent risk is reduced.

Answer: (SHOW ANSWER)

From a risk management perspective, the primary benefit of using automated system configuration validation tools is that they reduce the inherent risk, which is the risk that exists before any controls are applied. Automated system configuration validation tools can help to ensure that the system settings are consistent, compliant, and secure, and that they match the predefined standards and policies. This can reduce the likelihood and impact of errors, misconfigurations, vulnerabilities, or deviations that may compromise the system's functionality, performance, or integrity. The other options are not the primary benefits of using automated system configuration validation tools, although they may be secondary benefits or outcomes of doing so. Residual risk is the risk that remains after the controls are applied, and it may not be directly affected by the automated system configuration validation tools. Staff costs and operational costs are related to the efficiency and economy of the system configuration process, but they are not the main risk management objectives. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk Response, page 150.

NEW QUESTION: 637

Which of the following will BEST mitigate the risk associated with IT and business misalignment?

A. Establishing business key performance indicators (KPIs)

B. Introducing an established framework for IT architecture

C. Establishing key risk indicators (KRIs)

D. Involving the business process owner in IT strategy

Answer: (SHOW ANSWER)

IT and business misalignment is the risk that the IT objectives, plans, and activities are not aligned with the business goals, needs, and expectations. This can result in wasted resources, missed opportunities, poor performance, and customer dissatisfaction. One of the best ways to mitigate this risk is to involve the business process owner in IT strategy. The business process owner is the person who has the authority and responsibility for a specific business process and its outcomes. By involving the business process owner in IT strategy, the organization can ensure that the IT initiatives and solutions are relevant, effective, and beneficial for the business process and its stakeholders. The business process owner can also provide valuable input, feedback, and support for the IT strategy and its implementation. The other options are not the best ways to mitigate the risk associated with IT and business misalignment, although they may be helpful and complementary. Establishing business key performance indicators (KPIs) is a technique to measure and monitor the achievement of business objectives and outcomes. However, KPIs do not necessarily ensure that the IT strategy is aligned with the business strategy or that the IT activities support the business activities.

Introducing an established framework for IT architecture is a method to design and implement the IT infrastructure, systems, and services in a consistent and coherent manner. However, an IT architecture framework does not guarantee that the IT architecture is aligned with the business architecture or that the IT capabilities meet the business requirements. Establishing key risk indicators (KRIs) is a tool to monitor and communicate the level of exposure to a given risk or the potential impact of a risk. However, KRIs do not directly address the risk of IT and business misalignment or the actions needed to align them. References = CRISC Review Manual, pages 22-231; CRISC Review Questions, Answers & Explanations Manual, page 76

NEW QUESTION: 638
Which of the following has the GREATEST impact on backup policies for a system supporting a critical process?
A. Resource requirements of the process
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Impact of threats to the process
Answer: (SHOW ANSWER)

NEW QUESTION: 639
Which of the following is a risk practitioner's BEST course of action when a control is not meeting agreed-upon performance criteria?
A. Implement additional controls to further mitigate risk
B. Review performance results with the control owner
C. Redefine performance criteria based on control monitoring results
D. Recommend a tool to meet the performance requirements
Answer: (SHOW ANSWER)
The best approach is tocollaborate with the control ownerto understand root causes and determine next steps.
This respects ownership and enables targeted, informed decision-making before implementing drastic changes.
Reference:CRISC Manual - Domain 4, Slide 390-392

NEW QUESTION: 640
Which of the following is MOST helpful in providing an overview of an organization's risk management program?
Freecram.net
A. Risk scenarios
B. Risk management framework
C. Risk assessment results
D. Risk management treatment plan
Answer: (SHOW ANSWER)

The risk management framework defines the structure, objectives, roles, processes, and tools used by an organization to manage risk. It provides a comprehensive overview of how the enterprise governs and implements risk management.
According to the CRISC Review Manual and ISACA's Risk IT Framework:
"A risk management framework establishes and maintains a common risk language, defines principles and responsibilities, and ensures consistency of approach across the enterprise." While risk scenarios and assessment results are components of the program, they focus on specific areas.
The framework gives a holistic view-showing policies, processes, oversight mechanisms, governance linkages, and continuous improvement processes.
Hence, the Risk Management Framework (Option B) best provides an overview of the entire program.
CRISC Reference: Domain 1 - IT Risk Governance, Topic: Risk Management Framework and Governance Alignment.

NEW QUESTION: 641
Which of the following risk impacts should be the PRIMARY consideration for determining recovery priorities in a disaster recovery situation?
A. Data security
B. Recovery costs
C. Business disruption
D. Recovery resource availability
Answer: (SHOW ANSWER)
The primary consideration for determining recovery priorities in a disaster recovery situation is the impact of business disruption on the organization's mission, objectives, and stakeholders. Business disruption can result in loss of revenue, reputation, customer satisfaction, market share, and competitive advantage. Therefore, the recovery priorities should be based on the criticality of the business processes and functions that support the organization's value proposition and strategic goals. Data security (A), recovery costs (B), and recovery resource availability (D) are important factors, but they are secondary to the impact of business disruption.
Data security should be ensured throughout the recovery process, but it does not determine the recovery order.
Recovery costs should be balanced with the benefits of restoring the business operations, but they do not reflect the urgency of the recovery. Recovery resource availability should be assessed and allocated according to the recovery priorities, but it does not define the recovery sequence. (Risk and Information Systems Control Review Questions, Answers & Explanations Manual, 5th Edition, page 982)

NEW QUESTION: 642
An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?
A. Require the vendor to degauss the hard drives
B. Implement an encryption policy for the hard drives.
C. Require confirmation of destruction from the IT manager.

D. Use an accredited vendor to dispose of the hard drives.

Answer: (SHOW ANSWER)

Data leakage is the unauthorized or accidental disclosure of sensitive or confidential data to unauthorized parties. Data leakage can cause serious damages or losses to the organization, such as data breaches, fines, lawsuits, reputational harm, or loss of customer trust. Data leakage can occur due to various reasons, such as human errors, malicious attacks, or inadequate controls1.

An organization that uses a vendor to destroy hard drives faces a risk of data leakage, as the vendor may not properly or securely destroy the hard drives, or may access or misuse the data stored on them. The best way to reduce this risk is to use an accredited vendor to dispose of the hard drives, because it means that the vendor:

Has been certified or verified by a reputable or recognized authority or organization, such as ISACA, NAID, or R2, to provide hard drive destruction services Follows the industry standards and best practices for hard drive destruction, such as NIST 800-88 or DoD

5220.22-M, and ensures the compliance with the legal and regulatory requirements, such as HIPAA, PCI DSS, or GDPR Provides a secure and transparent process for hard drive destruction, such as using a specialized shredder, issuing a certificate of destruction, or allowing the customer to witness the destruction Maintains a high level of professionalism and integrity, and does not compromise the confidentiality or security of the customer's data234 The other options are not the best ways to reduce the risk of data leakage, but rather some of the steps or aspects of hard drive destruction. Require the vendor to degauss the hard drives is a step that can help to erase the data on the hard drives by using a strong magnetic field. However,degaussing may not be effective or reliable for some types of hard drives, such as solid state drives (SSDs), and it may not prevent the vendor from accessing or misusing the data before degaussing5. Implement an encryption policy for the hard drives is an aspect that can help to protect the data on the hard drives by using a cryptographic algorithm to make it unreadable without a key. However, encryption may not be sufficient or applicable for some types of data, such as metadata, and it may not prevent the vendor from accessing or misusing the key or the encrypted data6. Require confirmation of destruction from the IT manager is a step that can help to verify that the hard drives have been destroyed by the vendor, and to document the process and the outcome. However, confirmation of destruction may not be accurate or authentic, and it may not prevent the vendor from accessing or misusing the data before destruction7.

References = Data Leakage - ISACA Hard Drive Shredding Services | Hard Drive Destruction & Disposal Hard Drive Shredding and Destruction Service | CompuCycle Electronic Destruction & Recycling | Shred Nations Degaussing - ISACA Encryption - ISACA Certificate of Destruction - ISACA

[CRISC Review Manual, 7th Edition]

NEW QUESTION: 643

Which of the following is the GREATEST concern associated with insufficient focus on addressing blockchain interoperability in the SDLC?

A. Limited blockchain adoption and support

B. Reduced transaction speed and system responsiveness

C. Reduced network integrity and availability

D. Limited integration with external systems and blockchains

Answer: (SHOW ANSWER)

Limited integration with external systems and blockchainsis the greatest concern. Without considering interoperability during the SDLC, the system may not be able to connect seamlessly with partners or external networks, hindering business goals and limiting the blockchain's benefits.

NEW QUESTION: 644

An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

A. Number of customer records held

B. Number of databases that host customer data

C. Number of encrypted customer databases

D. Number of staff members having access to customer data

Answer: (SHOW ANSWER)

The best input to assess the inherent risk impact of leakage of customer data is the number of customer records held. Inherent risk impact is a measure of the potential severity or consequence of a risk event, before considering the existing controls. Inherent risk impact can be based on quantitative or qualitative factors, such as financial, operational, reputational, or legal factors. The number of customer records held is the best input, because it directly reflects the amount and type of data that could be leaked, and the potential harm or loss that could result from the leakage. The number of customer records held can also help to estimate the probability and frequency of the leakage, as well as the effectiveness and efficiency of the controls. The more customer records the organization holds, the higher the inherent risk impact of leakage, and the more controls the organization needs to implement and maintain. The other options are not the best input, although they may be related or influential to the inherent risk impact. The number of databases that host customer data is a measure of the complexity or diversity of the data storage and management systems, but it does not directly indicate the amount or type of data that could be leaked, or the potential harm or loss that could result from the leakage. The number of databases that host customer data may also vary depending on the design and configuration of the systems, which may not reflect the inherent risk impact. The number of encrypted customer databases is a measure of the security or protection of the data storage and management systems, but it is not an input to the inherent risk impact, rather it is an output or a result of the control implementation.

The number of encrypted customer databases may also depend on the quality and reliability of the encryption methods and keys, which may not indicate the inherent risk impact. The number of staff members having access to customer data is a measure of the exposure or vulnerability of the data to internal threats, such as unauthorized or malicious actions by the staff members. The number of staff members having access to customer data can affect the inherent risk impact, but it is not the best input, as it does not account for the external threats, such as hackers or competitors, or the amount or type of data that could be leaked, or the potential harm or loss that could result from the leakage. References = What is Inherent Risk? You Could Be at Risk of a Data Breach | UpGuard, Data leakage: A data leak is an unintentional exposure of sensitive data on the internet. For example, an employee might upload customer data files to an unsecured server. Lack of encryption: This is the storing, sending, or transferring information without converting it into ciphertext first.

NEW QUESTION: 645
Which of the following emerging technologies is frequently used for botnet distributed denial of service (DDoS) attacks?
A. Internet of Things (IoT)
B. Quantum computing
C. Virtual reality (VR)
D. Machine learning
Answer: (SHOW ANSWER)
Internet of Things (IoT) is an emerging technology that refers to the network of devices, such as cameras, sensors, appliances, or vehicles, that can communicate and exchange data via the internet. IoT is frequently used for botnet distributed denial of service (DDoS) attacks, which are cyberattacks that aim to disrupt or disable a target's online services by overwhelming them with traffic from multiple sources. IoT devices are often unsecured, unpatched, or misconfigured, which makes them vulnerable to being infected by malware and controlled by attackers. Attackers can use IoT devices to create large and powerful botnets that can launch DDoS attacks against various targets, such as websites, servers, or networks. According to the CRISC Review Manual 2022, IoT is one of the key emerging technologies that pose new IT risks, including DDoS attacks1.
According to the CRISC Review Questions, Answers & Explanations Manual 2022, IoT is the correct answer to this question2. According to the web search results, IoT devices are commonly used for botnet DDoS attacks, such as the Mirai botnet, the Emotet botnet, and the BoT-IoT dataset345.

NEW QUESTION: 646
Which of the following is the MOST efficient method for monitoring control effectiveness?
A. Conduct control self-assessments (CSAs)
B. Review system performance logs
C. Compare controls to business metrics
D. Perform independent periodic control testing
Answer: A (LEAVE A REPLY)
Control Self-Assessments (CSAs)provide an efficient way for process owners and staff to assess control effectiveness continuously. ISACA recognizes CSAs as a proactive approach that encourages accountability and early detection of control weaknesses, reducing the need for frequent external testing.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 647
Which of the following is MOST likely to be identified from an information systems audit report?
A. Resiliency
B. Regulatory requirements
C. Data ownership
D. Vulnerabilities
Answer: (SHOW ANSWER)
Information systems audits are designed to evaluate the effectiveness of controls and identify weaknesses or vulnerabilities within systems. Identifying vulnerabilities allows organizations to address potential security issues proactively.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Information Systems Auditing.

NEW QUESTION: 648
An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?
A. Third-party data custodian
B. Data custodian
C. Regional office executive
D. Data owner
Answer: (SHOW ANSWER)
The data owner is accountable for the confidentiality of the data that is outsourced to a third party with servers located in a foreign country. The data owner is the person or entity that has the authority and responsibility to classify, label, and protect the data according to the organization's policies and standards. The data owner is also responsible for defining the data access rights and privileges, and for ensuring that the data is handled in compliance with the applicable laws and regulations. The data owner retains the accountability for the data even when it is outsourced to a third party, and must monitor and evaluate the security performance and compliance of the service provider. The third-party data custodian, the data custodian, and the regional office executive are not accountable for the confidentiality of the data, as they have different roles and responsibilities in the outsourcing process. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.2.1.2, page 2461
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 654.

NEW QUESTION: 649
Which of the following is MOST important to sustainable development of secure IT services?
A. Security training for systems development staff
B. \Well-documented business cases
C. Security architecture principles
D. Secure coding practices
Answer: (SHOW ANSWER)

The most important factor for sustainable development of secure IT services is security training for systems development staff. Security training helps to ensure that the staff members are aware of the security risks, requirements, and best practices that affect the IT services they develop. Security training also helps to improve the security skills and knowledge of the staff members, and to foster a security culture and behavior within the development team. Security training can also help to prevent or reduce security defects, vulnerabilities, or incidents in the IT services, and to enhance the security performance and quality of the IT services. Well-documented business cases, security architecture principles, and secure coding practices are also important factors for sustainable development of secure IT services, but they are not as important as security training for systems development staff. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.1.1.2, page 2291
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 653.

NEW QUESTION: 650

Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

Freecram.net

A. Control owner
B. Risk owner
C. Internal auditor
D. Compliance manager
Answer: (SHOW ANSWER)
The internal auditor is the best suited to provide objective input when updating residual risk to reflect the results of control effectiveness. The internal auditor is an independent and impartial function that evaluates the adequacy and effectiveness of the internal controls and reports on the findings and recommendations. The internal auditor can provide an unbiased and reliable assessment of the residual risk, which is the risk that remains after the controls are applied. The other options are not as objective as the internal auditor, as they may have vested interests or conflicts of interest in the control environment. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Assessment, Section 2.4: IT Risk Response, page 87.

NEW QUESTION: 651
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?
A. Monitor processes to ensure recent updates are being followed.
B. Communicate to those who test and promote changes.
C. Conduct a cost-benefit analysis to justify the cost of the control.
D. Assess the maturity of the change management process.
Answer: (SHOW ANSWER)
* A change management process is a set of procedures and activities that ensure that any changes to the IT systems or applications are planned, approved, tested, implemented, and documented in a consistent and controlled manner.

* A change management process has recently been updated with new testing procedures. This means that the process has been improved or modified to include new or additional steps or methods for verifying and validating the changes before they are deployed to the production environment.
* The next course of action after updating the change management process with new testing procedures is to communicate to those who test and promote changes. This means that the change management team or function should inform and educate the people who are involved or affected by the changes, such as the developers, testers, users, customers, etc., about the new testing procedures, their purpose, benefits, requirements, and expectations.
* Communicating to those who test and promote changes helps to ensure that the new testing procedures are understood and followed by all the parties, that the changes are tested and promoted in accordance with the process standards and criteria, and that the changes are delivered with the expected quality and performance.
* The other options are not the next courses of action after updating the change management process with new testing procedures. They are either secondary or not essential for change management.
The references for this answer are:
* Risk IT Framework, page 27
* Information Technology & Security, page 21
* Risk Scenarios Starter Pack, page 19

NEW QUESTION: 652
Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?
A. Evaluating the impact to control objectives
B. Conducting a root cause analysis
C. Validating the adequacy of current processes
D. Reconfiguring the IT infrastructure
Answer: (SHOW ANSWER)
Conducting a root cause analysis is the best course of action for an IT business owner following an unexpected increase in emergency changes, as it helps to identify and address the underlying cause(s) of the problem and prevent it from recurring in the future. A root cause analysis is a systematic process of finding and resolving the fundamental factors that contribute to a specific issue or event. A root cause analysis can help to improve the quality and reliability of the IT services and processes, reduce the costs and risks associated with emergency changes, and enhance the customer satisfaction and trust.
The other options are not the best courses of action for an IT business owner following an unexpected increase in emergency changes. Evaluating the impact to control objectives is an important step to assess the potential consequences of the emergency changes on the IT governance and risk management, but it does not provide a solution or mitigation strategy for the problem. Validating the adequacy of current processes is a good practice to ensure that the IT processes are aligned with the business needs and objectives, but it does not address the specific cause(s) of the emergency changes. Reconfiguring the IT infrastructure is a possible action to implement the emergency changes, but it does not prevent the occurrence or recurrence of the problem. References = IT Business Owner's Best Course of Action Following

Unexpected Increase ..., ITIL Change Types: Standard vs Normal vs Emergency - Freshworks, Emergency Change Management: Please Stop The Drama

NEW QUESTION: 653
After several security incidents resulting in significant financial losses, IT management has decided to outsource the security function to a third party that provides 24/7 security operation services. Which risk response option has management implemented?
A. Risk mitigation
B. Risk avoidance
C. Risk acceptance
D. Risk transfer
Answer: (SHOW ANSWER)
Risk transferinvolves shifting the responsibility for managing specific risks to a third party. By outsourcing the security function, the organization transfers the associated risk to a vendor specializing in security management.

NEW QUESTION: 654
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?
A. Requiring the use of virtual private networks (VPNs)
B. Establishing a data classification policy
C. Conducting user awareness training
D. Requiring employee agreement of the acceptable use policy
Answer: (SHOW ANSWER)
The most effective way to mitigate the risk of unintentional data disclosure through the use of social media sites is to conduct user awareness training. User awareness training is a process of educating and informing the users about the security policies, procedures, and practices that are relevant and applicable to their roles and responsibilities. User awareness training can help to increase the knowledge, understanding, and compliance of the users regarding the data protection and privacy requirements, and the potential risks and consequences of data disclosure through social media sites. User awareness training can also help to influence the behavior, attitude, and culture of the users toward data security and privacy. The other options are not as effective as conducting user awareness training, as they are related to the technical, procedural, or contractual measures to mitigate the risk, not the human or behavioral measures to mitigate the risk. References = Risk and Information Systems Control Study Manual, Chapter 3: IT Risk Response, Section 3.3: IT Risk Response Implementation, page 145.

NEW QUESTION: 655
Which of the following should be of MOST concern to a risk practitioner reviewing the system development life cycle (SDLC)?
A. Testing is completed in phases, with user testing scheduled as the final phase.
B. Segregation of duties controls are overridden during user testing phases.

C. Data anonymization is used during all cycles of end-user testing.
D. Testing is completed by IT support users without input from end users.
Answer: (SHOW ANSWER)
Testing is completed by IT support users without input from end users should be of most concern to a risk practitioner reviewing the system development life cycle (SDLC). This is because testing without input from end users can result in poor quality, usability, and functionality of the system, as well as increased errors, defects, and rework. Testing without input from end users can also lead to user dissatisfaction, resistance, and non-compliance, as well as misalignment with the business requirements and objectives. According to the CRISC Review Manual 2022, one of the key risk identification techniques for IT projects is to involve the end users and other relevant parties in the testing process1. According to the CRISC Review Questions, Answers
& Explanations Manual 2022, testing without input from end users is the correct answer to this question2. Testing in phases, overriding segregation of duties controls, and using data anonymization are not the most concerning issues for a risk practitioner reviewing the SDLC. These are possible practices or techniques that can be used in the testing process, but they do not necessarily pose significant risks or problems. Testing in phases can help ensure that the system meets the technical and functional specifications, as well as the user acceptance criteria, at each stage of the development. Overriding segregation of duties controls can be justified and authorized during the testing phases, as long as the controls are restored and verified before the system goes live. Using data anonymization can help protect the privacy and security of the data used in the testing process, as well as comply with the relevant regulations and standards.

NEW QUESTION: 656
Which of the following is the MOST important reason for integrating IT risk management practices into enterprise risk management (ERM)?
A. To reduce conflicts of interest between IT and business units
B. To align ERM with regulatory requirements
C. To optimize enterprise-wide resource efficiency
D. To ensure IT risk scenarios are reflected in the corporate risk profile
Answer: (SHOW ANSWER)
IT risk is a subset of enterprise risk. Integration ensures IT risks are visible and prioritized alongside strategic and operational risks.
CRISC framework explains:
"Integration of IT risk management with ERM ensures that technology-related risks are appropriately represented in the overall corporate risk profile and reporting structure." Hence, D is correct.
CRISC Reference: Domain 1 - IT Risk Governance, Topic: Enterprise and IT Risk Integration.

NEW QUESTION: 657
Which of the following is the MOST important consideration for prioritizing risk treatment plans when faced with budget limitations?
A. Inherent risk and likelihood
B. Management action plans associated with audit findings

C. Residual risk relative to appetite and tolerance
D. Key risk indicator (KRI) trends
Answer: (SHOW ANSWER)
When prioritizing risk treatment plans under budget constraints, the focus should be onresidual risk relative to appetite and tolerance. This ensures that resources are allocated to risks that exceed the organization's risk appetite, aligning treatment efforts with strategic objectives and minimizing critical exposure.

NEW QUESTION: 658
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?
A. Increase in mitigating control costs
B. Increase in risk event impact
C. Increase in risk event likelihood
D. Increase in cybersecurity premium
Answer: (SHOW ANSWER)
The result of a significant increase in the motivation of a malicious threat actor would be an increase in risk event likelihood. The likelihood of a risk event is influenced by the factors of threat, vulnerability, and exposure. The motivation of a threat actor is a key component of the threat factor, as it reflects the intent and capability of the actor to exploit a vulnerability. Therefore, a higher motivation would imply a higher probability of an attack. An increase in mitigating control costs, risk event impact, or cybersecurity premium are possible consequences of a risk event, but they are not directly affected by the motivation of the threat actor. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 6; CRISC Review Manual, 6th Edition, page 67.

NEW QUESTION: 659
A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?
A. The alternative site is a hot site with equipment ready to resume processing immediately.
B. The contingency plan provides for backup media to be taken to the alternative site.
C. The contingency plan for high priority applications does not involve a shared cold site.
D. The alternative site does not reside on the same fault to matter how the distance apart.
Answer: (SHOW ANSWER)
A contingency plan is a set of actions and procedures that aim to ensure the continuity of critical business functions in the event of a disruption or disaster. An alternate processing site is a location where the organization can resume its information systems operations in case the primary site is unavailable or damaged. The most important consideration when establishing a contingency plan and an alternate processing site for a company located on a moderate earthquake fault is to ensure that the alternative site does not reside on the same fault, no matter how far apart they are. This is because an earthquake can affect a large area along the fault line, and potentially damage both the primary and the alternative site, rendering them unusable. By choosing an alternative site that is not on the same fault, the company can reduce the risk of losing both sites, and increase the likelihood of restoring its operations quickly and

effectively. The other options are not as important as the alternative site location, because they do not address the main threat of an earthquake, but rather focus on specific or partial aspects of the contingency plan, as explained below:
A: The alternative site is a hot site with equipment ready to resume processing immediately is a consideration that relates to the availability and readiness of the alternative site, but it does not ensure that the site is safe and secure from an earthquake. A hot site is a type of alternative site that has the necessary hardware, software, and network components to resume the information systems operations with minimal or no downtime. However, if the hot site is on the same fault as the primary site, it may not be accessible or functional after an earthquake, and the company may lose both sites and the data stored on them.
B: The contingency plan provides for backup media to be taken to the alternative site is a consideration that relates to the integrity and recoverability of the data, but it does not ensure that the site is safe and secure from an earthquake. Backup media are devices or systems that store copies of the data and information that are essential for the organization's operations. Taking backup media to the alternative site can help the company to restore its data and resume its operations in case the primary site is damaged or destroyed. However, if the alternative site is on the same fault as the primary site, it may not be accessible or functional after an earthquake, and the company may lose both sites and the backup media.
C: The contingency plan for high priority applications does not involve a shared cold site is a consideration that relates to the performance and reliability of the alternative site, but it does not ensure that the site is safe and secure from an earthquake. A shared cold site is a type of alternative site that has the necessary space and infrastructure to accommodate the information systems operations, but does not have the hardware, software, or network components installed. A shared cold site is shared by multiple organizations, and may not be available or suitable for the company's high priority applications, which require more resources and customization. However, if the alternative site is on the same fault as the primary site, it may not be accessible or functional after an earthquake, and the company may lose both sites and the ability to resume its high priority applications. References = Risk and Information Systems Control Study Manual, Chapter 4, Section
4.2.1, page 115. How to conduct a contingency planning process - IFRC, CP-4(2): Alternate Processing Site - CSF Tools - Identity Digital, Information System Contingency Planning Guidance - ISACA

NEW QUESTION: 660

Which of the following is the MOST important benefit of reporting risk assessment results to senior management?

Freecram.net

A. Promotion of a risk-aware culture
B. Compilation of a comprehensive risk register
C. Alignment of business activities
D. Facilitation of risk-aware decision making
Answer: (SHOW ANSWER)
Reporting risk assessment results to senior management is an essential part of risk communication, which is the process of sharing relevant and timely information about the risk exposure and risk management activities with the stakeholders. The most important benefit of reporting risk assessment results to senior management is to facilitate risk-aware decision making, which is the process of incorporating the risk

information and analysis into the strategic and operational decisions of the organization. By reporting the risk assessment results, the risk practitioner can provide senior management with the insight and understanding of the current and potential risks, their likelihood and impact, their interrelationships and dependencies, and their alignment with the risk appetite and tolerance. This can help senior management to prioritize the risks, allocate the resources, select the risk responses, monitor the risk performance, and evaluate the risk outcomes. References = CRISC Review Manual, 7th Edition, page 105.

NEW QUESTION: 661
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?
A. Logs and system events
B. Intrusion detection system (IDS) rules
C. Vulnerability assessment reports
D. Penetration test reports
Answer: (SHOW ANSWER)
The analysis of logs and system events will best help validate whether suspicious network activity is malicious, because they provide detailed and timely information about the source, destination, content, and context of the network traffic. Logs and system events can be collected from various sources, such as firewalls, routers, switches, servers, applications, and endpoints, and can be correlated and analyzed using tools such as security information and event management (SIEM) systems. By analyzing logs and system events, an organization can identify anomalies, patterns, trends, and indicators of compromise (IOCs) that may signal malicious network activity, such as unauthorized access, data exfiltration, malware infection, denial-of-service attack, or lateral movement. Logs and system events can also help determine the scope, impact, and root cause of the malicious network activity, and support the incident response and remediation process. References = Risk IT Framework, ISACA, 2022, p. 221

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 662
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?
A. Updating the risk register to include the risk mitigation plan
B. Determining processes for monitoring the effectiveness of the controls
C. Ensuring that control design reduces risk to an acceptable level
D. Confirming to management the controls reduce the likelihood of the risk

Answer: (SHOW ANSWER)

The primary focus of a risk owner once a decision is made to mitigate a risk is to ensure that the control design reduces the risk to an acceptable level. This means that the risk owner should verify that the control objectives, specifications, and implementation are aligned with the risk mitigation plan, and that the control is effective in reducing the risk exposure to within the risk appetite and tolerance of the enterprise. The risk owner should also ensure that the control design is consistent with the enterprise's policies, standards, and procedures, and that it complies with any relevant laws, regulations, or contractual obligations. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.4, page 185.

NEW QUESTION: 663

While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

A. Ensuring the vendor does not know the encryption key

B. Engaging a third party to validate operational controls

C. Using the same cloud vendor as a competitor

D. Using field-level encryption with a vendor supplied key

Answer: A (LEAVE A REPLY)

Encryption is a technique that transforms data into an unreadable format using a secret key, so that only authorized parties can access and decrypt the data. Encryption can help to protectsensitive data from unauthorized access or disclosure, especially when the data is stored or transmitted in the cloud1.

Ensuring the vendor does not know the encryption key is a control that will best reduce the risk associated with a data breach, because it can help to:

Prevent the vendor from accessing or disclosing the sensitive data, intentionally or unintentionally Limit the exposure or impact of the data breach, even if the vendor's systems or networks are compromised by hackers or malicious insiders Maintain the confidentiality and integrity of the sensitive data, regardless of the vendor's liability or responsibility Enhance the trust and confidence of the customers and stakeholders, who may be concerned about the vendor' s refusal to accept liability for a data breach23 The other options are not as effective as ensuring the vendor does not know the encryption key for reducing the risk associated with a data breach. Engaging a third party to validate operational controls is a control that can help to verify and improve the vendor's security practices and processes, but it does not guarantee that the vendor will prevent or respond to a data breach adequately or timely. Using the same cloud vendor as a competitor is not a control, but rather a business decision that may increase the risk associated with a data breach, as the vendor may have access to or disclose the sensitive data of both parties, or may favor one party over the other. Using field-level encryption with a vendor supplied key is a control that can help to encrypt specific fields or columns of data, such as names, addresses, or credit card numbers, but it does not prevent the vendor from accessing or disclosing the data, as the vendor has the encryption key4. References = Encryption - ISACA Cloud Encryption: Using Data Encryption in The Cloud Cloud Encryption: Why You Need It and How to Do It Right Field-Level Encryption - ISACA

[CRISC Review Manual, 7th Edition]

NEW QUESTION: 664
Which of the following is the BEST key control indicator (KCI) for measuring the security of a blockchain network?
A. Number of active nodes
B. Blockchain size in gigabytes
C. Average transaction speed
D. Number of validated transactions
Answer: (SHOW ANSWER)
The number of validated transactions is a critical indicator of a blockchain network's security. It reflects the network's ability to accurately and securely process transactions, ensuring data integrity and trustworthiness. A higher number of validated transactions indicates robust consensus mechanisms and effective security controls within the blockchain infrastructure.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: Key Control Indicators.

NEW QUESTION: 665
When assigning control ownership, it is MOST important to verify that the owner has accountability for:
A. Control effectiveness.
B. The budget for control implementation.
C. Assessment of control risk.
D. Internal control audits.
Answer: (SHOW ANSWER)
Control owners must be accountable for ensuring the effectiveness of the controls they manage. This accountability ensures the alignment of controls with risk objectives, as outlined in Control Governance and Ownership.

NEW QUESTION: 666
Which of the following is MOST important to consider when assessing the likelihood that a recently discovered software vulnerability will be exploited?
A. The skill level required of a threat actor
B. The amount of personally identifiable information (PH) disclosed
C. The ability to detect and trace the threat action
D. The amount of data that might be exposed by a threat action
Answer: A (LEAVE A REPLY)
When assessing the likelihood that a recently discovered software vulnerability will be exploited, the most important consideration is the skill level required of a threat actor. Here's an explanation:
* Skill Level of Threat Actors:
* The skill level required to exploit a vulnerability determines how accessible the exploit is to potential attackers.
* If a vulnerability requires advanced technical skills to exploit, it is less likely to be targeted by less sophisticated attackers.

* Conversely, if the exploit can be easily executed with minimal skills, it increases the likelihood of widespread exploitation.
* Factors Influencing Likelihood of Exploitation:
* Availability of Exploit Tools: If automated tools or scripts are available to exploit the vulnerability, even less skilled attackers can take advantage of it.
* Publication of Exploit Details: If the vulnerability and its exploitation method are widely published, it becomes more accessible to a broader range of attackers.
* Assessment of Likelihood:
* Security teams assess the skill level required by analyzing whether the exploit is straightforward or complex.
* They also consider the presence of exploit kits in the wild that could lower the barrier to entry for potential attackers.
* Comparison with Other Factors:
* Amount of PII Disclosed: While important, it relates more to the impact rather than the likelihood of exploitation.
* Ability to Detect and Trace: This is crucial for response but does not directly influence the likelihood of exploitation.
* Amount of Data Exposed: Similar to PII, this factor pertains to the impact rather than the likelihood of exploitation.
* References:
* The CRISC Review Manual discusses the importance of understanding the threat landscape, including the skill level of potential attackers (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.2.1 Internal Threats).

NEW QUESTION: 667
A risk practitioner is organizing risk awareness training for senior management. Which of the following is the MOST important topic to cover in the training session?
A. The organization's strategic risk management projects
B. Senior management roles and responsibilities
C. The organizations risk appetite and tolerance
D. Senior management allocation of risk management resources
Answer: C (LEAVE A REPLY)
The organization's risk appetite and tolerance are the most important topics to cover in a risk awareness training for senior management. Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk tolerance is the level of variation from the risk appetite that the organization is prepared to accept. Senior management plays a key role in defining and communicating the risk appetite and tolerance, as well as ensuring that they are aligned with the organization's strategy, culture, and values. By covering these topics in the training session, the risk practitioner can help senior management understand and articulate the risk preferences and boundaries of the organization, as well as monitor and adjust them as needed. The other options are not the most important topics to cover in a risk awareness training for senior management, although they may be relevant and useful. The organization's

strategic risk management projects are specific initiatives or activities that aim to identify, assess, and treat risks that may affect the organization's objectives. Senior management roles and responsibilities are the duties and expectations that senior management has in relation to risk management, such as providing leadership, oversight, and support.
Senior management allocation of risk management resources is the process of assigning and prioritizing the human, financial, and technical resources that are needed to implement and maintain risk management activities. These topics are more operational and tactical than strategic and may vary depending on the context and scope of the risk management function. References = CRISC Review Manual, pages 40-411; CRISC Review Questions, Answers & Explanations Manual, page 732

NEW QUESTION: 668
Which of the following is MOST useful when performing a quantitative risk assessment?
A. Management support
B. Industry benchmarking
C. Financial models
D. RACI matrix
Answer: (SHOW ANSWER)

NEW QUESTION: 669
Which of the following should be the PRIMARY objective of a risk awareness training program?
A. To enable risk-based decision making
B. To promote awareness of the risk governance function
C. To clarify fundamental risk management principles
D. To ensure sufficient resources are available
Answer: A (LEAVE A REPLY)
The primary objective of a risk awareness training program is to enable risk-based decision making, which means making decisions that take into account the potential risks and opportunities associated with each option. A risk awareness training program should aim to develop a common understanding of risk across multiple functions and business units, achieve a better understanding of risk for competitive advantage, and build safeguards against earnings-related surprises1. A risk awareness training program should also cover the basics of risk management, such as the risk management process, the roles and responsibilities of different stakeholders, the risk appetite and tolerance of the organization, and the tools and techniques for identifying, analyzing, evaluating, and treating risks234. A risk awareness training program should also include practical examples and case studies to illustrate how risk management can be applied in different scenarios and contexts5. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.11: Risk Awareness, pp. 34-354

NEW QUESTION: 670
Which of the following is MOST critical when designing controls?
A. Involvement of internal audit
B. Involvement of process owner

C. Quantitative impact of the risk
D. Identification of key risk indicators
Answer: B (LEAVE A REPLY)
The most critical factor when designing controls is the involvement of the process owner, who is the person responsible for the performance and outcomes of a business process. The process owner has the best knowledge and understanding of the process objectives, activities, inputs, outputs, resources, and risks. The process owner can provide valuable input and feedback on the design of controls that are relevant, effective, efficient, and aligned with the process goals. The process owner can also ensure that the controls are implemented, monitored, and improved as needed. The involvement of the process owner can also increase the acceptance and ownership of the controls by the process participants and stakeholders. The other options are less critical when designing controls. The involvement of internal audit can provide assurance and advice on the adequacy and effectiveness of the controls, but internal audit is not responsible for the design or implementation of the controls. The quantitative impact of the risk can help to prioritize and justify the controls, but it is not sufficient to determine the appropriate type and level of controls. The identification of key risk indicators can help to monitor and measure the risk and the performance of the controls, but it is not the main driver of the control design. References = Risk IT Framework, ISACA, 2022, p. 181

NEW QUESTION: 671
Who is the MOST appropriate owner for newly identified IT risk?
A. The manager responsible for IT operations that will support the risk mitigation efforts
B. The individual with authority to commit organizational resources to mitigate the risk
C. A project manager capable of prioritizing the risk remediation efforts
D. The individual with the most IT risk-related subject matter knowledge
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, the risk owner is the person who has the authority and accountability to manage a specific risk and its associated controls1. The risk owner is also responsible for ensuring that the risk is within the acceptable level and that the risk response is effective and efficient2. Therefore, the most appropriate owner for a newly identified IT risk is the individual who has the authority to commit organizational resources to mitigate the risk, as they have the most interest and influence on the risk and its impact on the business objectives. The other options are not the most appropriate owners for a newly identified IT risk, as they may not have the authority or the accountability to manage the risk. The manager responsible for IT operations that will support the risk mitigation efforts may have the operational responsibility or the oversight of the risk management activities, but they may not have the authority to allocate the resources or approve the risk response. A project manager capable of prioritizing the risk remediation efforts may have the project management skills or the knowledge of the risk management process, but they may not have the accountability or the ownership of the risk or its outcomes. The individual with the most IT risk-related subject matter knowledge may have the technical expertise or the understanding of the risk and its causes, but they may not have the decision-making power or the responsibility to manage the risk or its controls. References = CRISC Review Manual, pages 32-331; CRISC Review Questions, Answers & Explanations Manual, page 822

NEW QUESTION: 672
Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?
A. The cloud environment's capability maturity model
B. The cloud environment's risk register
C. The cloud computing architecture
D. The organization's strategic plans for cloud computing
Answer: (SHOW ANSWER)
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud computing architecture is the structure and design of the cloud environment, which includes the components, services, interfaces, standards, and configurations. The cloud computing architecture should be used as the primary basis for evaluating the state of an organization's cloud computing environment against leading practices, as it determines the performance, security, reliability, scalability, and interoperability of the cloud services. By comparing the cloud computing architecture with the best practices and benchmarks in the industry, an organization can identify the gaps and weaknesses in the cloud environment and implement the necessary improvements and controls. References = CRISC Review Manual, 7th Edition, page 156.

NEW QUESTION: 673
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?
A. Compliance breaches are addressed in a timely manner.
B. Risk ownership is identified and assigned.
C. Risk treatment options receive adequate funding.
D. Residual risk is within risk tolerance.
Answer: (SHOW ANSWER)
Risk treatment options are the actions or plans that are implemented to modify or reduce the risk exposure of the organization. Risk treatment options receive adequate funding when the organization allocates sufficient resources and budget to support the risk response actions, and to ensure that the risk controls are effective and efficient. This is the best evidence that risk management is driving business decisions in the organization, as it shows that the organization prioritizes and values the risk management process, and that it aligns its risk strategy and objectives with its business goals and value creation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 245. CRISC:
Certified in Risk & Information Systems Control Sample Questions, Question 245. CRISC Sample Questions 2024, Question 245.

NEW QUESTION: 674
Who is responsible for IT security controls that are outsourced to an external service provider?
A. Organization's information security manager

B. Organization's risk function
C. Service provider's IT management
D. Service provider's information security manager
Answer: (SHOW ANSWER)
The organization's information security manager is responsible for IT security controls that are outsourced to an external service provider. The information security manager is accountable for ensuring that the security policies and standards of the organization are followed by the service provider, and that the security objectives and requirements are met. The information security manager is also responsible for monitoring and evaluating the security performance and compliance of the service provider, and for managing the security risks and incidents that may arise from the outsourcing arrangement. The organization's risk function, the service provider's IT management, and the service provider's information security manager are not responsible for IT security controls that are outsourced, as they have different roles and responsibilities in the outsourcing process. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter
5, Section 5.2.1.2, page 2461
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 651.

NEW QUESTION: 675
The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:
A. rectify errors in results of KRIs.
B. detect changes in the risk profile.
C. reduce costs of risk mitigation controls.
D. continually improve risk assessments.
Answer: (SHOW ANSWER)
The primary reason for periodically monitoring key risk indicators (KRIs) is to detect changes in the risk profile of the enterprise. KRIs are metrics that provide information on the level of exposure to a specific risk or a group of risks. By monitoring KRIs, the enterprise can identify any deviations from the expected risk level, and take appropriate actions to adjust the risk response or the risk appetite. Monitoring KRIs also helps to validate the effectiveness of risk mitigation controls and the accuracy of risk assessments. Rectifying errors in results of KRIs, reducing costs of risk mitigation controls, and continually improving risk assessments are possible benefits of monitoring KRIs, but they are not the primary reason. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.1.1.2, page 175.

NEW QUESTION: 676
A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?
A. Aggregated key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Centralized risk register

D. Risk heat map

Answer: (SHOW ANSWER)

A risk heat map is a graphical tool that displays the overall risk of the project to senior management by showing the probability and impact of individual risks in a matrix format. A risk heat map can help to prioritize the risks, communicate the risk exposure, and monitor the risk response. A risk heat map can also show the risk appetite and tolerance levels of the organization, as well as the residual risk after the risk response. The other options are not the most effective ways to represent the overall risk of the project to senior management, although they may be useful or complementary to the risk heat map. Aggregated key performance indicators (KPIs) are metrics that measure the performance of the project against the objectives, but they do not show the uncertainty or variability of the project outcomes. Key risk indicators (KRIs) are metrics that measure the level of risk or the effectiveness of the risk response, but they do not show the relationship between the probability and impact of the risks. A centralizedrisk register is a document that records the details of the individual risks, such as the description, category, cause, effect, probability, impact, response, and status, but it does not show the overall risk of the project in a visual or concise way. References = Managing overall project risk, Project Risk Management - Quick Reference Guide, 10 Common Project Risks (Plus the Steps To Solve Them), What Is Project Risk Management: Benefits, Challenges, Best Practices

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 677

Which of the following is the MOST important responsibility of a business process owner to enable effective IT risk management?

A. Delivering risk reports in a timely manner

B. Prioritizing risk for appropriate response

C. Collecting and analyzing risk data

D. Escalating risk to senior management

Answer: (SHOW ANSWER)

NEW QUESTION: 678

Which of the following is the PRIMARY reason to conduct risk assessments at periodic intervals?

A. To ensure emerging risk is identified and monitored

B. To establish the maturity level of risk assessment processes

C. To promote a risk-aware culture among staff

D. To ensure risk trend data is collected and reported

Answer: (SHOW ANSWER)

NEW QUESTION: 679
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?
A. Recovery time objectives (RTOs)
B. Segregation of duties
C. Communication plan
D. Critical asset inventory
Answer: (SHOW ANSWER)
The most important information to cover in a business continuity awareness training program for all employees of the organization is the communication plan. A communication plan is a document that defines the roles, responsibilities, procedures, and resources for communicating with the internal and external stakeholders before, during, and after a business continuity event. A communication plan helps to ensure that the relevant and accurate information is delivered to the appropriate parties in a timely and consistent manner, and that the feedback and responses are received and addressed accordingly. A communication plan also helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal or regulatory requirements. A communication plan is the most important information to cover in a business continuity awareness training program, because it helps to prepare and educate the employees on how to communicate effectively and efficiently in a business continuity event, and how to avoid or minimize the communication errors, gaps, or conflicts that could affect the business continuity performance and recovery.
The other options are not as important as the communication plan, although they may also be covered in a business continuity awareness training program. Recovery time objectives (RTOs), segregation of duties, and critical asset inventory are all factors that could affect the business continuity planning and implementation, but they are not the most important information to cover in a business continuity awareness training program. References = 6

NEW QUESTION: 680
In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?
Freecram.net
A. The control catalog
B. The asset profile
C. Business objectives
D. Key risk indicators (KRIs)
Answer: (SHOW ANSWER)
In addition to the risk register, which is a tool to document and monitor the risks that affect the organization, a risk practitioner should review the business objectives of the organization to develop an understanding of its risk profile. The risk profile is a description of the set of risks that the organization faces in relation to its goals and strategies. By reviewing the business objectives, the risk practitioner can identify the sources, drivers, and consequences of the risks, as well as the alignment, prioritization, and tolerance of the risks. The

business objectives also provide the context and criteria for evaluating and managing the risks. The other options are not the best choices to review for developing an understanding of the organization's risk profile, as they do not capture the full scope and nature of the risks. The control catalog is a list of the existing controls that are implemented to mitigate the risks, but it does not reflect the effectiveness, efficiency, or sufficiency of the controls. The asset profile is a description of the resources and capabilities that the organization possesses or relies on, but it does not indicate the value, vulnerability, or interdependency of the assets. The key risk indicators (KRIs) are metrics that measure the level and trend of the risks, but they do not explain the causes, impacts, or responses to the risks. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.2, Page 49.

NEW QUESTION: 681

Which of the following is the BEST indication of a mature organizational risk culture?

A. Corporate risk appetite is communicated to staff members.

B. Risk owners understand and accept accountability for risk.

C. Risk policy has been published and acknowledged by employees.

D. Management encourages the reporting of policy breaches.

Answer: (SHOW ANSWER)

Organizational risk culture is the term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose. Organizational risk culture influences how the organization identifies, assesses, and manages risks, and how it aligns its risk appetite and tolerance with its objectives and strategies1.

The best indication of a mature organizational risk culture is that risk owners understand and accept accountability for risk, because it means that the organization:

Clearly defines and assigns the roles and responsibilities of the risk owners, who are the individuals or groups who have the authority and ability to manage the risks within their scope or domain Empowers and supports the risk owners to perform their risk management duties, such as identifying, assessing, responding, monitoring, and reporting the risks Holds the risk owners accountable for the outcomes and consequences of the risks, and evaluates their performance and compliance with the risk policies, standards, and procedures Encourages and rewards the risk owners for demonstrating risk awareness and competence, and for contributing to the risk management improvement and learning23 The other options are not the best indications of a mature organizational risk culture, but rather some of the elements or aspects of it. Corporate risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives. Corporate risk appetite is communicated to staff members to guide their risk decision making and behavior, and to ensure the consistency and alignment of the risk taking and tolerance across the organization. Risk policy is the document that establishes the principles, framework, and process for managing the risks within the organization. Risk policy is published and acknowledged by employees to ensure their awareness and compliance with the risk management expectations and requirements. Management is the group of individuals who have the authority and responsibility to direct and control the organization's activities and resources. Management encourages the reporting of policy breaches to ensure the transparency and accountability of the risk management performance and outcomes, and to identify and

address the risk management issues and gaps4. References = Risk culture - Institute of Risk Management Risk Owner - ISACA Taking control of organizational risk culture | McKinsey
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 682
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?
A. The value at which control effectiveness would fail
B. Thresholds benchmarked to peer organizations
C. A typical operational value
D. A value that represents the intended control state
Answer: (SHOW ANSWER)
A critical threshold value for a key control indicator (KCI) is the value that indicates that the control is no longer performing its intended function of mitigating a risk. If the KCI reaches or exceeds this value, it means that the control effectiveness has failed and corrective actions are needed. The other options are not the best representations of a critical threshold value for a KCI, because they do not reflect the actual performance or outcome of the control. Thresholds benchmarked to peer organizations, a typical operational value, and a value that represents the intended control state are examples of target or acceptable values for a KCI, not critical or unacceptable values. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 683
Which of the following is MOST important to consider when determining the risk associated with re-identification of obfuscated personal data?
A. The type of shared data
B. The level of residual risk after data loss prevention (DLP) controls are implemented
C. The monetary value of the unique records that could be re-identified
D. The impact to affected stakeholders
Answer: (SHOW ANSWER)
The impact to affected stakeholdersis the most critical factor when considering risks tied to re-identification. ISACA notes that risk is ultimately measured by how it affects stakeholders-including customers, partners, and regulators-particularly when personal data is involved.

NEW QUESTION: 684
Which of the following is the BEST approach for obtaining management buy-in to implement additional IT controls?
A. List requirements based on a commonly accepted IT risk management framework.
B. Provide information on new governance, risk, and compliance (GRC) platform functionalities.
C. Describe IT risk impact on organizational processes in monetary terms.
D. Present new key risk indicators (KRIs) based on industry benchmarks.
Answer: (SHOW ANSWER)

Presenting the impact of IT risks on organizational processes in monetary terms is effective for obtaining management buy-in because it directly relates to the organization's financial health and decision-making. It provides a clear and tangible understanding of the potential financial implications of risks, making it easier for management to appreciate the need for additional controls.

NEW QUESTION: 685
Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?
A. Requiring a printer access code for each user
B. Using physical controls to access the printer room
C. Using video surveillance in the printer room
D. Ensuring printer parameters are properly configured
Answer: (SHOW ANSWER)
The best control to prevent the inappropriate disclosure of confidential information when print jobs containing confidential information are sent to a shared network printer located in a secure room is to require a printer access code for each user. A printer access code is a unique and secret code that the user needs to enter on the printer device to release and retrieve the print job. Requiring a printer access code for each user is the best control, as it helps to prevent or limit the unauthorized access, viewing, or copying of the confidential information on the print job, especially if the print job is left unattended or forgotten on the printer device. Requiring a printer access code for each user also helps to ensure the accountability and traceability of the user who sent the print job, and to support the audit and monitoring of the printer activity. Using physical controls to access the printer room, using video surveillance in the printer room, and ensuring printer parameters are properly configured are also useful controls, but they are not as effective as requiring a printer access code for each user, as they do not directly prevent or limit the inappropriate disclosure of confidential information on the print job, and they may not deter or detect the unauthorized access or misuse of the print job by the authorized users who have access to the printer room or device. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 686
Which of the following is the MOST important key risk indicator (KRI) to protect personal information on corporate mobile endpoints?
A. Percentage of endpoints that are not encrypted
B. Number of endpoints not compliant with patching policy
C. Ratio of undiscoverable endpoints to encrypted endpoints
D. Percentage of endpoints with outdated antivirus signatures
Answer: (SHOW ANSWER)
Encryption statusdirectly relates to data confidentiality on mobile devices. ISACA emphasizes that data protection measures like encryption are critical controls for mitigating risks associated with mobile endpoints.

NEW QUESTION: 687

Which of the following would MOST likely drive the need to review and update key performance indicators (KPIs) for critical IT assets?

A. The outsourcing of related IT processes

B. Outcomes of periodic risk assessments

C. Changes in service level objectives

D. Findings from continuous monitoring

Answer: (SHOW ANSWER)

Key performance indicators (KPIs) are metrics used to measure and evaluate the achievement of the organization's objectives and strategies1. KPIs for critical IT assets are KPIs that focus on the performance and value of the IT assets that are essential for the organization's operations and functions2. KPIs for critical IT assets may include metrics such as availability, reliability, utilization, cost, and security of the IT assets3. The need to review and update KPIs for critical IT assets may be driven by various factors, such as changes in the business environment, customer expectations, or regulatory requirements. However, the most likely factor that would drive the need to review and update KPIs for critical IT assets is the outcomes of periodic risk assessments. A risk assessment is a process that involves identifying, analyzing, and evaluating the risks and their potential impacts on the organization's objectives and performance4. A periodic risk assessment is a risk assessment that is performed at regular intervals, such as monthly, quarterly, or annually, to capture the changes and updates in the risk environment and the risk profile5. The outcomes of periodic risk assessments would most likely drive the need to review and update KPIs for critical IT assets, as they would provide insights into the current and emerging risks that may affect the performance and value of the critical IT assets, as well as the effectiveness and efficiency of the existingand planned controls and responses. By reviewing and updating the KPIs for critical IT assets based on the outcomes of periodic risk assessments, the organization can ensure that the KPIs are relevant, realistic, and aligned with the organization's risk appetite and tolerance, and that they provide accurate and timely information for decision making and reporting. The outsourcing of related IT processes, changes in service level objectives, and findings from continuous monitoring are not the most likely factors that would drive the need to review and update KPIs for critical IT assets, as they do not provide the same level of information and impact as the outcomes of periodic risk assessments. The outsourcing of related IT processes is a decision that involves transferring some or all of the IT processes that support or enable the critical IT assets to an external service provider. The outsourcing of related IT processes may affect the performance and value of the critical IT assets, but it does not necessarily require a review and update of the KPIs for critical IT assets, as the KPIs may still be valid and applicable for the outsourced IT processes. Changes in service level objectives are changes in the expected or agreed level of quality or performance of the IT services that support or enable the critical IT assets. Changes in service level objectives may affect the performance and value of the critical IT assets, but they do not necessarily require a review and update of the KPIs for critical IT assets, as the KPIs may still be consistent and compatible with the changed service level objectives. Findings from continuous monitoring are the results or outcomes of the ongoing observation and measurement of the performance and compliance of the IT processes and systems that support or enable the critical IT assets. Findings from continuous monitoring may affect the performance and value of the critical IT assets, but they do not necessarily require a review and update of the KPIs for critical IT assets, as the KPIs may still be relevant and reliable for the continuously monitored IT processes and systems. References = Risk and

Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.

NEW QUESTION: 688
The risk associated with an asset after controls are applied can be expressed as:
A. a function of the cost and effectiveness of controls.
B. the likelihood of a given threat.
C. a function of the likelihood and impact.
D. the magnitude of an impact.
Answer: (SHOW ANSWER)
The risk associated with an asset after controls are applied can be expressed as a function of the likelihood and impact, as it helps to measure and quantify the residual risk level and exposure. Residual risk is the risk that remains after the implementation of controls or risk treatments. Residual risk can be calculated by multiplying the likelihood and impact of a risk event, where likelihood is the probability or frequency of the risk event occurring, and impact is the consequence or severity of the risk event on the asset or objective. Residual risk can be expressed as:
ResidualRisk=Likelihood×Impact
Expressing the risk associated with an asset after controls are applied as a function of the likelihood and impact helps to provide the following benefits:
* It enables a data-driven and evidence-based approach to risk assessment and reporting, rather than relying on subjective or qualitative judgments.
* It facilitates a consistent and standardized way of measuring and communicating risk levels and exposure across the organization and to the external stakeholders.
* It supports the alignment of risk management and control activities with the organizational strategy and objectives, and helps to evaluate the achievement of the desired outcomes.
* It helps to identify and prioritize the areas for improvement and enhancement of the risk management and control processes, and guide the development and implementation of corrective or preventive actions.
* It provides feedback and learning opportunities for the risk management and control processes, and helps to foster a culture of continuous improvement and innovation.
The other options are not the best ways to express the risk associated with an asset after controls are applied.
A function of the cost and effectiveness of controls is a measure of the inputs or outputs of the risk management and control processes, but it does not indicate the risk level or exposure. The likelihood of a given threat is a component of the risk calculation, but it does not reflect the impact or consequence of the threat. The magnitude of an impact is a component of the risk calculation, but it does not reflect the likelihood or probability of the risk event. References = Risk Assessment and Analysis Methods: Qualitative and Quantitative, IT Risk Resources | ISACA, Residual Risk: Definition, Formula & Management - Video & Lesson ...

NEW QUESTION: 689

A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:
A. updating the risk register.
B. validating the risk scenarios.
C. documenting the risk scenarios.
D. identifying risk mitigation controls.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, the most important time to involve business stakeholders in the development of bottom-up IT risk scenarios is when validating the risk scenarios, as they can provide valuable input on the relevance, completeness, and accuracy of the scenarios and their impact on the business objectives and processes2
1: CRISC Review Questions, Answers & Explanations Database, Question ID: 100001 2: CRISC Review Manual, 7th Edition, page 97

NEW QUESTION: 690
A bank recently incorporated blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?
Freecram.net
A. be available to all stakeholders.
B. be reviewed by the IT steering committee.
C. effectively support a business maturity model.
D. reflect the results of risk assessments.
Answer: (SHOW ANSWER)

NEW QUESTION: 691
Which of the following has the GREATEST impact on ensuring the alignment of the risk profile with business objectives?
A. Stage gate reviews throughout the risk management process
B. Incorporation of industry best practice benchmarks and standards
C. Senior management approval of risk appetite and tolerance
D. An effective enterprise-wide risk awareness program
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 692

Which of the following BEST enables senior management to make risk treatment decisions in line with the organization's risk appetite?

A. Risk scenarios

B. Industry risk benchmarks

C. Quantitative risk analysis

D. Risk remediation plans

Answer: (SHOW ANSWER)

NEW QUESTION: 693

Which of the following should be management's PRIMARY consideration when approving risk response action plans?

A. Ability of the action plans to address multiple risk scenarios

B. Ease of implementing the risk treatment solution

C. Changes in residual risk after implementing the plans

D. Prioritization for implementing the action plans

Answer: (SHOW ANSWER)

The management's primary consideration when approving risk response action plans should be the changes in residual risk after implementing the plans. Residual risk is the level of risk that remains after the implementation of risk responses1. It indicates the degree of exposure or uncertainty that the organization still faces, and the potential impact or consequences of the risk events. The management should evaluate the effectiveness and adequacy of the risk responses, and decide whether the residual risk is acceptable or not2. The management should also compare the residual risk with the risk appetite, which is the amount and type of risk that the organization is willing to accept or pursue in order to achieve its objectives3. The management should ensure that the residual risk is aligned with the risk appetite, and that the risk responses are consistent and proportional to the risk level4.

The other options are not the primary consideration when approving risk response action plans, because:

* Ability of the action plans to address multiple risk scenarios is a desirable but not essential criterion for approving risk response action plans. Risk scenarios are hypothetical situations that describe how a risk event could occur and what the consequences could be5. They can help to understand and communicate the nature and impact of the risks, and to design and evaluate the risk responses6. However, not all risk scenarios are equally likely or relevant, and some risk scenarios may be too complex or improbable to address. Therefore, the ability of the action plans to address multiple risk scenarios is not the primary consideration, but rather a secondary or supplementary one.
* Ease of implementing the risk treatment solution is a practical but not critical criterion for approving risk response action plans. Risk treatment is the process of selecting and applying appropriate measures to modify the risk7. It can involve different strategies, such as avoid, reduce, transfer, or accept the risk8. The ease of implementing the risk treatment solution depends on various factors, such as the availability of resources, the feasibility of the solution, or the cooperation of the stakeholders. However, the ease of implementation is not the primary consideration, but rather a supporting or facilitating one.
* Prioritization for implementing the action plans is a useful but not vital criterion for approving risk response action plans. Prioritization is the process of ranking the action plans according to their importance, urgency,

or impact. It can help to allocate the resources, schedule the activities, and monitor the progress of the action plans. However, prioritization is not the primary consideration, but rather a subsequent or follow-up one.
References =
* Residual Risk - CIO Wiki
* What is Residual Risk? - Definition from Techopedia
* Risk Appetite - CIO Wiki
* Risk Appetite: What It Is and Why It Matters - Gartner
* Risk Scenarios Toolkit - ISACA
* Risk Scenarios Starter Pack - ISACA
* Risk Treatment - CIO Wiki
* Risk Treatment Plan - CIO Wiki
* [Prioritization - CIO Wiki]

NEW QUESTION: 694
When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?
A. Unclear organizational risk appetite
B. Lack of senior management participation
C. Use of highly customized control frameworks
D. Reliance on qualitative analysis methods
Answer: (SHOW ANSWER)
Senior management participation is essential for the success of an organization's risk management framework, as it demonstrates the commitment, support, and leadership for the risk management activities. Senior management participation also ensures that the risk management framework is aligned with the organization's strategy, objectives, and culture, and that the risk management roles and responsibilities are clearly defined and communicated. Senior management participation also facilitates the allocation of adequate resources, the establishment of risk appetite and tolerance, and the monitoring and reporting of risk performance. Therefore, the lack of senior management participation should be of greatest concern to a risk practitioner, as it indicates a low level of risk maturity and a high level of risk exposure. The other options are not as concerning as the lack of senior management participation, because they do not affect the risk management framework as significantly, and they can be addressed or improved with the involvement of senior management, as explained below:
A: Unclear organizational risk appetite is a deficiency that can affect the risk management framework, as it can lead to inconsistent or inappropriate risk decisions and responses. However, this deficiency can be resolved or mitigated with the participation of senior management, whocan define and communicate the risk appetite and tolerance for the organization, and ensure that they are aligned with the organization's strategy and objectives.
C: Use of highly customized control frameworks is a deficiency that can affect the risk management framework, as it can create complexity, confusion, or duplication in the control design and implementation.

However, this deficiency can be resolved or mitigated with the participation of senior management, who can review and rationalize the control frameworks, and ensure that they are relevant, effective, and efficient for the organization's risk profile and environment.
D: Reliance on qualitative analysis methods is a deficiency that can affect the risk management framework, as it can limit the accuracy, reliability, and comparability of the risk information and assessment. However, this deficiency can be resolved or mitigated with the participation of senior management, who can support and promote the use of quantitative analysis methods, such as the FAIR framework1, and provide the necessary data, tools, and skills for the risk analysis and evaluation. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.3.2, page 18.

NEW QUESTION: 695
A small organization finds it difficult to implement separation of duties necessary to mitigate the likelihood of system misuse. Which of the following would be the BEST compensating control?
A. Undertake control self-assessments (CSAs)
B. Require reports from staff with multiple duties
C. Obtain independent analysis of transaction logs
D. Assign activities to fewer employees
Answer: (SHOW ANSWER)
When separation of duties (SoD) cannot be fully implemented-typically due to limited personnel-a compensating control must provide comparable assurance that no individual can exploit a conflict of interest or perform unauthorized actions without detection.
According to the CRISC study guide and ISACA's Control Objectives for Information and Related Technologies (COBIT):
* Compensating controls substitute for missing primary controls when business or technical constraints prevent their full implementation.
* The most effective compensating control for SoD issues is independent review or monitoring of activities performed by those with multiple roles.
Obtaining an independent analysis of transaction logs ensures that another trusted party validates the actions taken by employees, detecting inappropriate or fraudulent activities.
Option explanations:
* A. Control self-assessments are self-reviews, not independent, and therefore insufficient for SoD conflicts.
* B. Reports from staff with multiple duties still depend on self-reporting, which lacks independence.
* D. Assigning activities to fewer employees increases risk rather than mitigating it.
This aligns with CRISC's emphasis that "an independent review of audit logs is the best compensating control when segregation of duties conflict exists in a small IT department." (CRISC Notes, Slide 349).

NEW QUESTION: 696
The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:
A. develop a comprehensive risk mitigation strategy
B. develop understandable and realistic risk scenarios
C. identify root causes for relevant events

D. perform an aggregated cost-benefit analysis

Answer: (SHOW ANSWER)

Low-probability, high-impact events are those that have a low chance of occurring but would cause significant harm if they do. These events are often difficult to predict and quantify, but they can have a major impact on the organization's objectives, reputation, or operations. By including these events in a risk assessment, the organization can develop understandable and realistic risk scenarios that reflect the potential consequences of different outcomes1. This can help the organization to prioritize its risk management activities and allocate its resources accordingly.

References = Risk and Information Systems Control Study Manual, Chapter 5: Risk Assessment Process

NEW QUESTION: 697

Which of the following is the MOST important course of action to foster an ethical, risk-aware culture?

A. Implement a fraud detection and prevention framework.

B. Ensure the alignment of the organization's policies and standards to the defined risk appetite.

C. Establish an enterprise-wide ethics training and awareness program.

D. Perform a comprehensive review of all applicable legislative frameworks and requirements.

Answer: (SHOW ANSWER)

According to the CRISC Review Manual, an enterprise-wide ethics training and awareness program is one of the key elements of a strong risk culture, as it helps to promote ethical behavior, raise awareness of risk management principles and practices, and foster a culture of accountability and transparency2

1: Developing Collective Risk Leadership Through CRISC - ISACA 2: CRISC Review Manual, 7th Edition, page 23

NEW QUESTION: 698

Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

A. Use production data in a non-production environment

B. Use masked data in a non-production environment

C. Use test data in a production environment

D. Use anonymized data in a non-production environment

Answer: (SHOW ANSWER)

Using anonymized data in a non-production environment is the best approach for an organization in a heavily regulated industry to comprehensively test application functionality. Anonymized data is data that has been stripped of any personally identifiable information (PII) or other sensitive data, such as names, addresses, phone numbers, email addresses, etc. Anonymized data protects the privacy and security of the data, while still preserving the structure and format of the original data. Using anonymized data in a non-production environment allows the organization to test the application functionality without risking data breaches or violating regulations. Using production data, masked data, or test data in either production or non-production environments are not as optimal as using anonymized data, because they may introduce errors, inconsistencies, or vulnerabilities in the data or the application. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.3.1, page 3-21.

NEW QUESTION: 699
A risk practitioner has just learned about new done FIRST?
A. Notify executive management.
B. Analyze the impact to the organization.
C. Update the IT risk register.
D. Design IT risk mitigation plans.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, impact analysis is the process of estimating and evaluating the potential effects of a risk event on the organization's objectives, processes, resources, and risks. Impact analysis helps to quantify and qualify the severity and likelihood of the risk, and to identify the possible consequences and implications for the organization. Impact analysis is the first step that should be done when a risk practitioner learns about a new threat, as it helps to assess the current level of risk exposure and the urgency of the risk response. Impact analysis also helps to communicate and report the risk to the relevant stakeholders, and to facilitate risk-based decision making and action planning. References = CRISC Review Manual1, page 208.

NEW QUESTION: 700
Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (IoT) technology in an organization?
Freecram.net
A. The business case for the use of IoT
B. The IoT threat landscape
C. Policy development for IoT
D. The network that IoT devices can access
Answer: (SHOW ANSWER)
* Risk scenarios: Narratives that describe potential risk events, their causes, consequences, and likelihood1.
* Internet of Things (IoT): A network of interconnected devices, software, sensors, and other things that communicate and exchange data without human intervention2.
* IoT threat landscape: The range and types of threats and attacks that target IoT devices, systems, and networks3.
The most helpful thing to review when identifying risk scenarios associated with the adoption of IoT technology in an organization is the IoT threat landscape. The IoT threat landscape provides a comprehensive and current overview of the potential sources, methods, and impacts of cyberattacks on IoT devices, systems, and networks. Reviewing the IoT threat landscape can help an organization to:
* Identify the most relevant and prevalent threats and vulnerabilities that affect IoT technology, such as weak passwords, insecure interfaces, insufficient data protection, poor device management, or lack of encryption4.
* Assess the likelihood and impact of different types of attacks, such as malware infections, denial-of-service attacks, data breaches, unauthorized access, or sabotage4.
* Prioritize the most critical and urgent risks that need to be addressed and mitigated.
* Develop realistic and plausible risk scenarios that reflect the actual IoT threat environment and the organization's specific context and objectives.

The other options are not as helpful as the IoT threat landscape when identifying risk scenarios associated with the adoption of IoT technology in an organization, because they do not provide a comprehensive and current view of the potential threats and attacks that target IoT technology. The business case for the use of IoT, which is the justification and rationale for adopting IoT technology based on the expected benefits, costs, and risks, may help to understand the value and purpose of IoT technology for the organization, but it does not provide detailed information on the specific threats and vulnerabilities that affect IoT technology. Policy development for IoT, which is the process of creating and implementing rules and guidelines for the governance, management, and security of IoT technology, may help to establish the standards and expectations for IoT technology within the organization, but it does not provide an overview of the external threats and attacks that target IoT technology. The network that IoT devices can access, which is the infrastructure and system that enables the connectivity and communication of IoT devices, may help to identify the potential entry points and attack vectors for IoT threats, but it does not provide a complete picture of the types and impacts of IoT threats.
References = Risk Scenarios Toolkit, What is the Internet of Things (IoT)? With Examples | Coursera, Top IoT security issues and challenges (2022) - Thales, 8 Internet of Things Threats and Security Risks - SecurityScorecard

NEW QUESTION: 701
When of the following 15 MOST important when developing a business case for a proposed security investment?
A. identification of control requirements
B. Alignment to business objectives
C. Consideration of new business strategies
D. inclusion of strategy for regulatory compliance
Answer: (SHOW ANSWER)
Alignment to business objectives is the most important factor when developing a business case for a proposed security investment, because it demonstrates how the investment will support the enterprise's mission, vision, and goals. A business case should show how the security investment will contribute to the value creation, risk reduction, and performance improvement of the enterprise. The other options are not the most important factors, although they may also be included in the business case. The identification of control requirements, the consideration of new business strategies, and the inclusion of strategy for regulatory compliance are secondary factors that depend on the alignment to business objectives. References = Most Asked CRISC Exam Questions and Answers

NEW QUESTION: 702
An organization needs to send files to a business partner to perform a quality control audit on the organization' s record-keeping processes. The files include personal information on the organization's customers. Which of the following is the BEST recommendation to mitigate privacy risk?
A. Obfuscate the customers' personal information.
B. Require the business partner to delete personal information following the audit.
C. Use a secure channel to transmit the files.

D. Ensure the contract includes provisions for sharing personal information.

Answer: (SHOW ANSWER)

Obfuscating customer information ensures data privacy by rendering sensitive details unintelligible to unauthorized parties, reducing the risk of exposure during transit or processing. This aligns withData Protection and Privacy Regulationsunder risk management frameworks, emphasizing safeguarding personally identifiable information.

NEW QUESTION: 703

A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

A. Risk avoidance

B. Risk transfer

C. Risk mitigation

D. Risk acceptance

Answer: (SHOW ANSWER)

The global organization has adopted risk acceptance as the risk response with regard to privacy requirements, as it has decided to continue with the implementation of the application that does not address all privacy requirements across multiple jurisdictions, and bear the potential consequences of noncompliance. Risk avoidance, risk transfer, and risk mitigation are not the risk responses adopted by the organization, as they would involve avoiding, sharing, or reducing the risk of noncompliance with privacy requirements, respectively. References = CRISC Review Manual, 7th Edition, page 111.

NEW QUESTION: 704

The PRIMARY benefit of maintaining an up-to-date risk register is that it helps to:

A. implement uniform controls for common risk scenarios.

B. ensure business unit risk is uniformly distributed.

C. build a risk profile for management review.

D. quantify the organization's risk appetite.

Answer: (SHOW ANSWER)

A risk register is a document that records and tracks the information and status of the identified risks and their responses. It includes the risk description, category, source, cause, impact, probability, priority, response, owner, action plan, status, etc.

A risk profile is a summary or representation of the organization's exposure or level of risk, based on the results of the risk assessment and evaluation. A risk profile can show the distribution and comparison of the risks based on various criteria, such as likelihood, impact, category, source, etc. A risk profile can also indicate the organization's risk appetite and tolerance, and the gaps or opportunities for improvement.

The primary benefit of maintaining an up-to-date risk register is that it helps to build a risk profile for management review, because it provides the data and information that are necessary and relevant for creating and updating the risk profile, and for communicating and reporting the risk profile to the management.

Maintaining an up-to-date risk register can help to build a risk profile for management review by providing the following benefits:
It can ensure that the risk profile reflects the current and accurate state and performance of the organization's risk management function, and that it covers all the relevant and significant risks that may affect the organization's objectives and operations.
It can provide useful references and benchmarks for the identification, analysis, evaluation, and communication of the risks and their responses, and for the alignment and integration of the risks and their responses with the organization's strategy and culture.
It can support the decision making and planning for the risk management function, and for the allocation and optimization of the resources, time, and budget for the risk management function.
The other options are not the primary benefits of maintaining an up-to-date risk register, because they do not address the main purpose and benefit of building a risk profile for management review, which is to summarize and represent the organization's exposure or level of risk, and to communicate and report it to the management.
Implementing uniform controls for common risk scenarios means applying and enforcing the same or similar controls or countermeasures for the risks that have the same or similar characteristics or features, such as source, cause, impact, etc. Implementing uniform controls for common risk scenarios can help to ensure the consistency and efficiency of the risk management function, but it is not the primary benefit of maintaining an up-to-date risk register, because it does not summarize or represent the organization's exposure or level of risk, and it may not be relevant or appropriate for the organization's objectives and needs.
Ensuring business unit risk is uniformly distributed means ensuring that the risks that are associated with the different business units or divisions of the organization are balanced or equalized, and that they do not exceed or fall below the organization's risk appetite and tolerance. Ensuring business unit risk is uniformly distributed can help to optimize the performance and profitability of the organization, but it is not the primary benefit of maintaining an up-to-date risk register, because it does not summarize or represent the organization' s exposure or level of risk, and it may not be feasible or realistic for the organization.
Quantifying the organization's risk appetite means measuring and expressing the amount and type of risk that the organization is willing and able to accept or take, in pursuit of its objectives and goals. Quantifying the organization's risk appetite can help to establish and communicate the boundaries and expectations for the organization's risk management function, but it is not the primary benefit of maintaining an up-to-date risk register, because it does not summarize or represent the organization's exposure or level of risk, and it may not be consistent or compatible with the organization's strategy and culture. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48, 54-55, 58-59, 62-63
ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 201 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 705
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?
A. Verbal majority acceptance of risk by committee

B. List of compensating controls
C. IT audit follow-up responses
D. A memo indicating risk acceptance
Answer: (SHOW ANSWER)
The strongest evidence to support a risk response decision is a memo indicating risk acceptance. A memo is a formal and written document that can clearly communicate the rationale, criteria, and approval of the risk acceptance decision. Verbal majority acceptance of risk by committee, list of compensating controls, and IT audit follow-up responses are weaker evidence, as they may not be documented, verified, or aligned with the risk response decision. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 11; CRISC Review Manual, 6th Edition, page 144.

NEW QUESTION: 706
Who should be PRIMARILY responsible for establishing an organization's IT risk culture?
A. Business process owner
B. Executive management
C. Risk management
D. IT management
Answer: (SHOW ANSWER)
Executive management should be primarily responsible for establishing an organization's IT risk culture, as they have the authority and accountability to define and communicate the vision, mission, values, and objectives of the organization, and to set the tone and direction for the IT risk management and control processes. Executive management is the highest level of management in an organization, and it consists of the board of directors, the chief executive officer (CEO), and other senior executives. Executive management is responsible for the strategic planning and decision making of the organization, and for ensuring the alignment of the organizational strategy and objectives with the stakeholder expectations and requirements. Executive management should be primarily responsible for establishing an organization's IT risk culture by providing the following benefits:
It demonstrates the leadership and commitment of the executive management to the IT risk management and control processes, and to the achievement of the organizational strategy and objectives.
It influences and motivates the behavior and attitude of the staff and managers towards IT risk management and control, and fosters a culture of risk awareness, ownership, and accountability across the organization.
It defines and communicates the IT risk appetite and tolerance of the organization, and guides and supports the development and implementation of the IT risk policies, standards, and procedures.
It allocates and monitors the resources and performance of the IT risk management and control processes, and ensures the effectiveness and efficiency of the IT risk governance and oversight.
The other options are not the primary choices for establishing an organization's IT risk culture. Business process owner is the person who has the responsibility and authority over the design, execution, and performance of a specific business process, and they are accountable for the risks and controls associated with their process, but they do not have the overall or strategic responsibility for the IT risk culture. Risk management is the function or department that is responsible for managing and monitoring the IT risk

management and control processes, and for providing advice and guidance to the executive management and the business units, but they do not have the ultimate or final responsibility for the IT risk culture. ITmanagement is the function or department that is responsible for managing and maintaining the IT operations and security, and for supporting the IT risk management and control processes, but they do not have the highest or broadest responsibility for the IT risk culture. References = Risk Culture - Open Risk Manual, IT Risk Resources | ISACA, The 6 key elements to creating and maintaining a good risk culture

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 707
Which of the following would provide the MOST comprehensive information for communicating current levels of IT-related risk to executive management?
A. Risk register
B. Risk appetite
C. Risk dashboard
D. Risk action plans
Answer: (SHOW ANSWER)
A risk dashboard provides a visual, real-time overview of risk levels, trends, and key metrics, making it easier for executive management to understand and act upon. It integrates data from various sources, making it comprehensive.
Reference:CRISC Manual - Domain 4, Slide 445-448

NEW QUESTION: 708
Which of the following is the MOST important consideration for a risk practitioner when making a system implementation go-live recommendation?
A. Completeness of system documentation
B. Results of end user acceptance testing
C. Variances between planned and actual cost
D. availability of in-house resources
Answer: (SHOW ANSWER)
End user acceptance testing is a process that verifies that a system or service meets the requirements and expectations of the end users, who are the actual or potential customers or beneficiaries of the system or service. End user acceptance testing is the final stage of testing before the system or service is deployed or released to the production environment. The results of end user acceptance testing are the most important consideration for a risk practitioner when making a system implementation go-live recommendation, as they

indicate the quality, functionality, usability, and reliability of the system or service from the end user perspective. The results of end user acceptance testing can help to identify and resolve any defects, errors, or issues that may affect the performance, satisfaction, or acceptance of the system or service by the end users.
The results of end user acceptance testing can also help to evaluate the benefits, value, and risks of the system or service for the end users and the organization. The other options are not the most important consideration for a risk practitioner when making a system implementation go-live recommendation, although they may be relevant and useful. The completeness of system documentation is a factor that affects the maintainability, supportability, and auditability of the system or service, but it does not measure the end user experience or satisfaction. The variances between planned and actual cost is a measure of the efficiency and budget management of the system or service development or implementation, but it does not reflect the end user needs or expectations. The availability of in-house resources is a resource that supports the system or service delivery and operation, but it does not ensure the end user acceptance or approval. References = CRISC Review Manual, pages 180-1811; CRISC Review Questions, Answers & Explanations Manual, page 87

NEW QUESTION: 709
A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?
A. The team that performed the risk assessment
B. An assigned risk manager to provide oversight
C. Action plans to address risk scenarios requiring treatment
D. The methodology used to perform the risk assessment
Answer: C (LEAVE A REPLY)
A risk register is a tool that records and tracks the risks that may affect a project, as well as the actions that are taken or planned to manage them1. A risk register should include information such as the risk description, category, source, impact, likelihood, severity, owner, status, and response2. Among these, the most important information to capture in the risk register is the action plans to address risk scenarios requiring treatment. This is because the action plans are the specific steps that are taken to reduce, avoid, transfer, or accept the risks, depending on thechosen risk treatment option3. The action plans should beclear, realistic, measurable, and aligned with the project objectives and constraints4. The action plans should also be monitored and updated regularly to ensure that they are effective and appropriate for the changing risk environment5. The action plans are essential for managing the risks and ensuring the successful delivery of the project. The other options are not the most important information to capture in the risk register, as they are either less relevant or less actionable than the action plans. The team that performed the risk assessment is the group of people who identified, analyzed, and evaluated the risks, using various tools and techniques6. While this information may be useful foraccountability and communication purposes, it is not as important as the action plans, as it does not indicate how the risks are treated or resolved. The assigned risk manager to provide oversight is the person who has the responsibility and authority to oversee the risk management process and ensure that the risks are properly identified, assessed, treated, and reported. While this information may be useful for governance and coordination

purposes, it is not as important as the action plans, as it does not specify what actions are taken or planned to manage the risks. The methodology used to perform the risk assessment is the approach or framework that is used to identify, analyze, and evaluate the risks, based on the project context, scope, and objectives. While this information may be useful for consistency and transparency purposes, it is not as important as the action plans, as it does not describe how the risks are addressed or mitigated. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section
2.1.5, Page 55.

NEW QUESTION: 710

Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

Freecram.net

A. To plan for the replacement of assets at the end of their life cycles
B. To assess requirements for reducing duplicate assets
C. To understand vulnerabilities associated with the use of the assets
D. To calculate mean time between failures (MTBF) for the assets
Answer: (SHOW ANSWER)
Understanding vulnerabilities associated with the use of the assets is the primary reason for a risk practitioner to review an organization's IT asset inventory, as it helps to identify and assess the potential threats and risks to the assets. The other options are not the primary reasons for a risk practitioner to review an organization's IT asset inventory, although they may be related to the process.

NEW QUESTION: 711
Who should have the authority to approve an exception to a control?
A. information security manager
B. Control owner
C. Risk owner
D. Risk manager
Answer: (SHOW ANSWER)
The control owner is the person who has the authority to approve an exception to a control. A control is a policy, procedure, or technical measure that is implemented to prevent or mitigate a risk. A control owner is responsible for the design, implementation, operation, and maintenance of the control, as well as for monitoring and reporting its performance and effectiveness. A control owner is also accountable for the approval of any changes or exceptions to the control, based on the risk assessment and business justification.
An information security manager, a risk owner, and a risk manager are not the best choices, as they do not have the same level of authority, responsibility, and knowledge as the control owner in relation to the control. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 35.

NEW QUESTION: 712
Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

A. Prioritizing risk within each business unit
B. Reviewing risk ranking methodology
C. Promoting an organizational culture of risk awareness
D. Assigning risk ownership to appropriate roles
Answer: (SHOW ANSWER)
The best way to ensure adequate resources will be allocated to manage identified risk is to assign risk ownership to appropriate roles. Risk ownership is the process of assigning the authority and responsibility to manage a specific risk or a group of related risks to a person or entity. Risk ownership helps to ensure adequate resources for managing risk, because it helps to define and clarify the roles and responsibilities of the risk owners, and to establish and enforce the expectations and standards for the risk owners. Risk ownership also helps to measure and evaluate the effectiveness and efficiency of the risk owners, and to identify and address any issues or gaps in the risk management activities. The other options are not as effective as assigning risk ownership to appropriate roles, although they may be related to the risk management process. Prioritizing risk within each business unit, reviewing risk ranking methodology, and promoting an organizational culture of risk awareness are all activities that can help to support or improve the risk management process, but they do not necessarily ensure adequate resources for managing risk.
References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.1, page 2-11.

NEW QUESTION: 713
Which of the following is the PRIMARY concern related to using pseudonymization for the protection of an organization's processed privacy data?
A. Authorized users can access personal data.
B. Updates to privacy data content are not allowed.
C. Individual data subjects can be re-identified.
D. Other information about the data subject can be revealed.
Answer: (SHOW ANSWER)
Pseudonymization replaces identifying fields in a data record with artificial identifiers or pseudonyms. However, unlike full anonymization, re-identification remains possible if the pseudonym can be matched with external or hidden reference data.
CRISC and privacy-risk guidance (aligned with GDPR principles) emphasize that:
"The primary concern when using pseudonymization as a privacy safeguard is the potential for re-identification of individual data subjects."
* Pseudonymized data can still be linked back to individuals if the mapping key or auxiliary datasets are compromised.
* True anonymization eliminates any reasonable means of re-identification, but pseudonymization does not.
* Therefore, while pseudonymization reduces exposure, it does not fully eliminate privacy risk.
Options A, B, and D are not inherent to pseudonymization:
* Authorized access and update restrictions are policy issues, not intrinsic to pseudonymization.
* Other information disclosure (D) could occur through inference but is secondary to direct re- identification.
Hence, C. Individual data subjects can be re-identified is the correct and verified answer as per CRISC and GDPR-aligned data protection practices.

NEW QUESTION: 714
Which stakeholder is MOST important to include when defining a risk profile during me selection process for a new third party application'?
A. The third-party risk manager
B. The application vendor
C. The business process owner
D. The information security manager
Answer: (SHOW ANSWER)
A risk profile is a summary of the nature and level of risk that an organization faces. It includes information such as the sources, causes, and consequences of the risks, their likelihood and impact, their interrelationships and dependencies, and their alignment with the risk appetite and tolerance. A risk profile is influenced by various factors, such as the organization's objectives, strategies, activities, processes, resources, capabilities, culture, etc. When defining a risk profile during the selection process for a new third party application, the stakeholder that is most important to include is the business process owner, who is the person who has the authority and responsibility for the design, execution, and performance of a business process. The business process owner can provide valuable input and insight into the requirements, expectations, and dependencies of the business process that will use the new third party application, and the potential risks and opportunities that may arise from the selection of the application. The business process owner can also help to prioritize and address the risks, and ensure that the risk profile is aligned with the business objectives and strategies. References = 5

NEW QUESTION: 715
Which of the following BEST indicates the condition of a risk management program?
A. Number of risk register entries
B. Number of controls
C. Level of financial support
D. Amount of residual risk
Answer: (SHOW ANSWER)
The best indicator of the condition of a risk management program is the amount of residual risk. Residual risk is the risk that remains after the implementation of risk responses. Residual risk reflects the effectiveness and efficiency of the risk management program in reducing the risk exposure to an acceptable level, and in aligning the risk profile with the risk appetite and tolerance of the enterprise. A low amount of residual risk indicates that the risk management program is performing well, and that the controls are adequate and appropriate. A high amount of residual risk indicates that the risk management program is not functioning properly, and that the controls are insufficient or ineffective. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.2.2, page 191

NEW QUESTION: 716
Which of the following is MOST important to include in a Software as a Service (SaaS) vendor agreement?
A. An annual contract review

B. A service level agreement (SLA)
C. A requirement to adopt an established risk management framework
D. A requirement to provide an independent audit report
Answer: (SHOW ANSWER)
A service level agreement (SLA) is a contract between a SaaS vendor and a customer that defines the quality and availability of the SaaS service, as well as the responsibilities and obligations of both parties. An SLA is most important to include in a SaaS vendor agreement because it sets the expectations and standards for the SaaS service, provides a mechanism for measuring and monitoring the service performance, and establishes the remedies and penalties for service failures or breaches. An SLA can also help to mitigate the risks and liabilities associated with SaaS delivery, such as data security, privacy, compliance, and disaster recovery.
The other options are not the most important to include in a SaaS vendor agreement, although they may be beneficial or desirable depending on the context and nature of the SaaS service. An annual contract review is a process of evaluating and revising the SaaS vendor agreement to reflect the changing needs and circumstances of the customer and the vendor, but it is not a mandatory or essential element of the agreement.
A requirement to adopt an established risk management framework is a way of ensuring that the SaaS vendor follows the best practices and standards for identifying, assessing, and mitigating the risks related to the SaaS service, but it is not a specific or measurable term of the agreement. A requirement to provide an independent audit report is a way of verifying and validating the SaaS vendor's compliance with the SLA and other contractual obligations, but it is not a direct or primary component of the agreement. References = SaaS Agreements: Key Contractual Provisions, SaaS Agreement: Everything You Need to Know, Essential checklist for SaaS agreement negotiations, Key Clauses To Understand and Evaluate in SaaS Contracts, SaaS Reseller Agreement: Everything You Need to Know

NEW QUESTION: 717
A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?
A. Conduct a gap analysis.
B. Terminate the outsourcing agreement.
C. Identify compensating controls.
D. Transfer risk to the third party.
Answer: (SHOW ANSWER)
The best course of action when a recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services is to conduct a gap analysis, as it involves comparing the current and desired states of compliance, and identifying any gaps or discrepancies that need to be addressed. Terminating the outsourcing agreement, identifying compensating controls, and transferring risk to the third party are not the best courses of action, as they may not be feasible, effective, or appropriate, respectively, and may require the prior knowledge of the compliance gaps and risks. References = CRISC Review Manual, 7th Edition, page 111.

NEW QUESTION: 718
A new software package that could help mitigate risk in an organization has become available. Which of the following is the risk practitioner's BEST course of action?
A. Perform a business impact analysis (BIA).
B. Perform a cost-benefit analysis.
C. Review industry best practice.
D. Review risk governance policies.
Answer: (SHOW ANSWER)
Cost-benefit analysis evaluates whether the benefits (e.g., risk reduction, efficiency) of implementing the new tool justify the costs (e.g., acquisition, maintenance). This analysis is critical for informed decision-making and resource optimization.
Reference:CRISC Manual - Domain 3, Slide 325, 303

NEW QUESTION: 719
Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?
A. Fiscal management practices
B. Business maturity
C. Budget for implementing security
D. Management culture
Answer: (SHOW ANSWER)
The most critical factor to consider when determining an organization's risk appetite is the management culture. The management culture reflects the values, beliefs, and attitudes of the senior management and the board of directors toward risk management. The management culture influences how the organization defines, communicates, and implements its risk appetite and tolerance. Fiscal management practices, business maturity, and budget for implementing security are other factors that may affect the risk appetite, but they are not as critical as the management culture. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 8; CRISC Review Manual, 6th Edition, page 97.

NEW QUESTION: 720
Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?
Freecram.net
A. Defining expectations in the enterprise risk policy
B. Increasing organizational resources to mitigate risks
C. Communicating external audit results
D. Avoiding risks that could materialize into substantial losses
Answer: (SHOW ANSWER)
According to the Risk Appetite vs. Risk Tolerance: What is the Difference? article, risk tolerance is the acceptable level of variation that an organization is willing to accept around a specific objective. Risk tolerance is usually expressed as a range or a limit, and it helps to guide the decision making and risk taking

of the organization. The best way to promote adherence to the risk tolerance level set by management is to define the expectations in the enterprise risk policy, which is a document that establishes the organization's risk management framework, principles, and objectives. By defining the expectations in the enterprise risk policy, the organization can communicate the risk tolerance level to all the relevant stakeholders, and ensure that they understand and follow the risk management guidelines and standards. This can help to create a consistent and coherent risk culture across the organization, and to avoid any deviations or violations of the risk tolerance level. References = Risk Appetite vs. Risk Tolerance: What is the Difference?

NEW QUESTION: 721
Which of the following should be the HIGHEST priority when developing a risk response?
A. The risk response addresses the risk with a holistic view.
B. The risk response is based on a cost-benefit analysis.
C. The risk response is accounted for in the budget.
D. The risk response aligns with the organization's risk appetite.
Answer: (SHOW ANSWER)
A risk response is the action or plan that is taken to address a specific risk that has been identified, analyzed, and evaluated. It can be one of the following types: mitigate, transfer, avoid, or accept.
The highest priority when developing a risk response is to ensure that it aligns with the organization's risk appetite, which is the amount and type of risk that the organization is willing to accept in pursuit of its goals. The risk appetite is usually expressed as a range or a threshold, and it is aligned with the organization's strategy and culture.
Aligning the risk response with the organization's risk appetite ensures that the risk response is consistent, appropriate, and proportional to the level and nature of the risk, and that it supports the organization's objectives and values. It also helps to optimize the balance between risk and return, and to create and protect value for the organization and its stakeholders.
The other options are not the highest priority when developing a risk response, because they do not address the fundamental question of whether the risk response is suitable and acceptable for the organization.
The risk response addresses the risk with a holistic view means that the risk response considers the interrelationships and dependencies among the risk sources, events, impacts, and responses, and the potential secondary and residual effects of the risk response. This is important to ensure that the risk response is comprehensive and effective, and that it does not create new or unintended risks, but it is not the highest priority when developing a risk response, because it does not indicate whether the risk response is aligned with the organization's risk appetite.
The risk response is based on a cost-benefit analysis means that the risk response compares the expected costs and benefits of implementing the risk response, and selects the risk response that provides the most favorable net outcome. This is important to ensure that the risk response is efficient and economical, and that it maximizes the return on investment, but it is not the highest priority when developing a risk response, because it does not indicate whether the risk response is aligned with the organization's risk appetite.
The risk response is accounted for in the budget means that the risk response is included in the financial plan and allocation of resources for the organization or the project. This is important to ensure that the risk response is feasible and realistic, and that it has the necessary funding and support, but it is not the highest

priority when developing a risk response, because it does not indicate whether the risk response is aligned with the organization's risk appetite. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 29-30, 34-35, 38-39, 44-45, 50-51, 54-55 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 147

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 722
Which of the following is MOST important when developing key performance indicators (KPIs)?
A. Alignment to risk responses
B. Alignment to management reports
C. Alerts when risk thresholds are reached
D. Identification of trends
Answer: (SHOW ANSWER)
* Key performance indicators (KPIs) are quantifiable measures of progress toward an intended result, such as a strategic objective or a desired outcome12.
* The most important factor when developing KPIs is the alignment to risk responses, which are the actions taken to address the risks that may affect the achievement of the intended result12.
* Alignment to risk responses means that the KPIs should reflect the effectiveness and efficiency of the risk responses, and provide feedback and guidance for improving the risk responses12.
* Alignment to risk responses also means that the KPIs should be consistent and compatible with the risk responses, and support the risk management process and objectives12.
* The other options are not the most important factor, but rather possible aspects or features of KPIs that may vary depending on the context and purpose of the KPIs. For example:
* Alignment to management reports is an aspect of KPIs that relates to the communication and presentation of the KPIs to the relevant stakeholders, such as senior management, board members, or external parties12. However, this aspect does not determine the quality or validity of the KPIs, or the alignment to the intended result12.
* Alerts when risk thresholds are reached is a feature of KPIs that relates to the monitoring and control of the KPIs, and the triggering of actions or decisions when the KPIs exceed or fall below a certain level or range12. However, this feature does not define the content or scope of the KPIs, or the alignment to the intended result12.
* Identification of trends is a feature of KPIs that relates to the analysis and interpretation of the KPIs, and the identification of patterns or changes in the KPIs over time or across different dimensions12. However, this

feature does not specify the criteria or methodology of the KPIs, or the alignment to the intended result12.
References =
* 1: What is a Key Performance Indicator (KPI)? Guide & Examples - Qlik3
* 2: What is a Key Performance Indicator (KPI)? - KPI.org4

NEW QUESTION: 723
Prior to selecting key performance indicators (KPIs), itis MOST important to ensure:
A. trending data is available.
B. process flowcharts are current.
C. measurement objectives are defined.
D. data collection technology is available.
Answer: (SHOW ANSWER)
* Key performance indicators (KPIs) are metrics that provide information about the achievement of specific goals or objectives.
* Prior to selecting KPIs, it is most important to ensure that measurement objectives are defined. This means that the desired outcomes and targets of the goals or objectives are clearly stated and aligned with the organization's strategy and vision.
* Defining measurement objectives helps to select the most relevant and meaningful KPIs that can accurately reflect the progress and performance of the goals or objectives. It also helps to establish the criteria and standards for evaluating and reporting the results and outcomes of the KPIs.
* The other options are not the most important things to ensure prior to selecting KPIs. They are either secondary or not essential for KPIs.
The references for this answer are:
* Risk IT Framework, page 16
* Information Technology & Security, page 10
* Risk Scenarios Starter Pack, page 8

NEW QUESTION: 724
Which of the following is the MOST important reason for a risk practitioner to continuously monitor a critical security transformation program?
A. To validate the quality of defined deliverables for the program
B. To detect increases in program costs
C. To ensure program risk events are mitigated in a timely manner
D. To provide timely reporting to the governance steering committee
Answer: (SHOW ANSWER)
Continuously monitoring a critical security transformation program is crucial for a risk practitioner primarily to ensure that any risk events are identified and mitigated promptly. This ensures that the security transformation remains on track and that potential risks do not escalate to a level that could compromise the program's success.
Identifying and Mitigating Risks:

Risk Identification:Continuously monitoring the program helps in the early identification of risks. This is essential because unidentified risks can lead to unexpected issues that might derail the program.
Timely Mitigation:Once risks are identified, it is crucial to mitigate them as quickly as possible. Delays in mitigation can allow risks to grow in impact, making them harder and more expensive to address.
Ensuring Program Continuity:
Maintaining Momentum:Security transformation programs often involve significant changes and can be disruptive. By ensuring that risks are mitigated in a timely manner, the risk practitioner helps maintain the program's momentum and keeps it on schedule.
Preventing Escalation:Timely risk mitigation prevents minor issues from escalating into major problems that could halt the program.
Aligning with Strategic Goals:
Strategic Alignment:Ensuring timely mitigation of risks helps in keeping the program aligned with the strategic goals of the organization. It ensures that the security objectives are met without significant delays or cost overruns.
References:
The importance of timely risk mitigation in program management is emphasized in various risk management frameworks and standards, such as the ISO 31000 and ISACA's Risk IT Framework. These frameworks highlight the need for ongoing risk monitoring and timely response to ensure successful program execution.

NEW QUESTION: 725
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?
A. Ask the business to make a budget request to remediate the problem.
B. Build a business case to remediate the fix.
C. Research the types of attacks the threat can present.
D. Determine the impact of the missing threat.
Answer: (SHOW ANSWER)
Determining the impact of the missing threat is the best course of action for a peer review of a risk assessment, as it helps to assess the potential consequences and severity of the threat on the information system and the business objectives. Determining the impact of the missing threat is a process of estimating and quantifying the possible harm or loss that could result from the occurrence of the threat event, such as data breach, system failure, or service disruption. Determining the impact of the missing threat can help to: Identify and prioritize the critical assets, processes, and functions that could be affected by the threat Evaluate and measure the extent and magnitude of the damage or disruption caused by the threat Analyze and compare the current and residual risk levels and control effectiveness Develop and implement appropriate risk response and mitigation strategies and actions Communicate and report the risk exposure and status to the relevant stakeholders Determining the impact of the missing threat is an essential step to ensure the completeness and accuracy of the risk assessment and to improve the quality and reliability of the risk management and control processes.

The other options are not the best courses of action for a peer review of a risk assessment. Asking the business to make a budget request to remediate the problem is a possible action to allocate the resources and costs for the risk mitigation, but it does not address the root cause or the severity of the problem. Building a business case to remediate the fix is a possible action to justify and support the risk mitigation, but it does not provide a clear and comprehensive analysis of the problem. Researching the types of attacks the threat can present is a possible action to understand and anticipate the threat scenarios andtechniques, but it does not evaluate the actual or potential impact of the threat. References = Risk Assessment and Analysis Methods: Qualitative and Quantitative, IT Risk Resources | ISACA, Peer Review Assessment Framework

NEW QUESTION: 726
Which of the following is the MOST significant risk related to an organization's use of AI technology?
A. The AI system's contract does not include a right-to-audit clause
B. The AI system is being used beyond its intended purpose
C. The AI system is on unsupported infrastructure
D. The AI system results have not been validated
Answer: (SHOW ANSWER)
Unvalidated AI outputs pose considerable integrity and operational risks, potentially leading to erroneous decisions or compliance lapses. ISACA CRISC guidance underscores that ensuring results validity is a highest-priority control for new technologies such as AI.

NEW QUESTION: 727
Which of the following would BEST help minimize the risk associated with social engineering threats?
A. Enforcing employees' sanctions
B. Conducting phishing exercises
C. Enforcing segregation of dunes
D. Reviewing the organization's risk appetite
Answer: (SHOW ANSWER)
Conducting phishing exercises would best help minimize the risk associated with social engineering threats, because they can help to raise awareness and educate employees about the common techniques and tactics used by social engineers, such as sending deceptive emails or text messages that ask for sensitive information or direct users to malicious websites. Phishing exercises are simulated attacks that test the employees' ability to recognize and respond to social engineering attempts, and provide feedback and guidance on how to improve their security behavior. By conducting phishing exercises, the organization can measure and improve the employees' level of security awareness and resilience, and reduce the likelihood and impact of falling victim to social engineering attacks. The other options are less effective ways to minimize the risk associated with social engineering threats. Enforcing employees' sanctions can help to deter and punish employees who violate the security policies or procedures, but it may not prevent or reduce the occurrence of social engineering attacks, as they may target employees who are unaware, careless, or coerced by the attackers.
Enforcing segregation of duties can help to prevent or limit the damage caused by social engineering attacks, by restricting the access and authority of employees to perform certain tasks or functions, but it may not

address the root cause or source of the attacks, which is the human factor. Reviewing the organization's risk appetite can help to define and communicate the amount and type of risk that the organization is willing to accept in pursuit of its objectives, but it may not directly affect or influence the employees' behavior or attitude toward social engineering threats, which may depend on their individual or situational factors. References = How to Prevent and Mitigate Social Engineering Attacks 1

NEW QUESTION: 728
Which of the following is the GREATEST benefit of using IT risk scenarios?
A. They support compliance with regulations.
B. They provide evidence of risk assessment.
C. They facilitate communication of risk.
D. They enable the use of key risk indicators (KRIs)
Answer: C (LEAVE A REPLY)
The greatest benefit of using IT risk scenarios is that they facilitate communication of risk, as they provide a clear and realistic description of the risk sources, events, impacts, and responses, and enable the stakeholders to understand and appreciate the risk exposure and appetite of the organization. Supporting compliance with regulations, providing evidence of risk assessment, and enabling the use of key risk indicators (KRIs) are also benefits of using IT risk scenarios, but they are not the greatest benefit, as they are more related to the outcomes or consequences of risk communication, rather than the process or value of risk communication. References = CRISC Review Manual, 7th Edition, page 100.

NEW QUESTION: 729
An IT license audit has revealed that there are several unlicensed copies of co be to:
A. immediately uninstall the unlicensed software from the laptops
B. centralize administration rights on laptops so that installations are controlled
C. report the issue to management so appropriate action can be taken.
D. procure the requisite licenses for the software to minimize business impact.
Answer: (SHOW ANSWER)
An IT license audit is a process that verifies the compliance of the IT software and hardware assets with the licensing agreements and regulations. An IT license audit can reveal the existence of unlicensed copies of software, which can expose the enterprise to legal, financial, and reputational risks. The best course of action in such a situation is to report the issue to management so that appropriate action can be taken. Management can then decide on the most suitable risk response strategy, such as procuring the necessary licenses, uninstalling the unlicensed software, or negotiating with the software vendor. Reporting the issue to management can also help to prevent further violations, identify the root causes, and implement corrective and preventive measures. The other options are not the best course of action, as they may not address the issue effectively, efficiently, or ethically. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.1.1, pp. 156-157.

NEW QUESTION: 730

Which of the following provides The BEST information when determining whether to accept residual risk of a critical system to be implemented?

freecram.net

A. Single loss expectancy (SLE)
B. Cost of the information system
C. Availability of additional compensating controls
D. Potential business impacts are within acceptable levels
Answer: (SHOW ANSWER)
The BEST information when determining whether to accept residual risk of a critical system to be implemented is the potential business impacts are within acceptable levels, because it indicates that the residual risk, which is the risk that remains after the risk response actions, does not exceed the risk tolerance and appetite of the organization, and that it does not pose a significant threat or disruption to the business objectives and processes. The potential business impacts are the consequences or outcomes of the residual risk on the organization's performance, reputation, and value. The other options are not as informative as the potential business impacts, because:
Option A: Single loss expectancy (SLE) is a measure of the monetary loss that is expected from a single occurrence of a risk event, but it does not provide the best information when determining whether to accept residual risk, because it does not consider the frequency or probability of the risk event, or the qualitative aspects of the risk impact, such as customer satisfaction, employee morale, or regulatory compliance.
Option B: Cost of the information system is a measure of the total expenditure that is required to acquire, develop, operate, and maintain the information system, but it does not provide the best information when determining whether to accept residual risk, because it does not reflect the value or benefit of the information system, or the risk exposure or variation that the information system may introduce or encounter.
Option C: Availability of additional compensating controls is a measure of the alternative or supplementary controls that can be implemented to reduce the residual risk, but it does not provide the best information when determining whether to accept residual risk, because it does not indicate the effectiveness or efficiency of the compensating controls, or the cost-benefit analysis of implementing them. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 122.

NEW QUESTION: 731
An organization plans to provide specific cloud security training for the IT team to help manage risks associated with cloud technology. This response is considered risk:
A. Transfer
B. Mitigation
C. Acceptance
D. Deferral
Answer: (SHOW ANSWER)
Risk mitigation involves implementing measures to reduce either the likelihood or impact of a risk.
By providing targeted training, the organization increases staff capability, thereby reducing the likelihood of misconfigurations or compliance errors in cloud usage.
ISACA defines mitigation as:
"Implementing controls or training to reduce exposure to risk within acceptable levels."

* A Transfer = insurance or outsourcing.
* C Acceptance = no action.
* D Deferral = postponing response.
Hence, B. Mitigation is correct.
CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Risk Response Options.

NEW QUESTION: 732
A migration from an in-house developed system to an external cloud-based solution is affecting a previously rated key risk scenario related to payroll processing. Which part of the risk register should be updated FIRST?
A. Payroll system risk factors
B. Payroll system risk mitigation plans
C. Payroll process owner
D. Payroll administrative controls
Answer: (SHOW ANSWER)
Payroll system risk mitigation plans are the actions that are taken to reduce or eliminate the risk associated with payroll processing. When a migration from an in-house developed system to an external cloud-based solution is affecting a previously rated key risk scenario related to payroll processing, the first part of the risk register that should be updated is the payroll system risk mitigation plans. This is because the migration may introduce new risks or change the existing risks, and the risk mitigation plans may need to be revised or replaced accordingly. Updating the payroll system risk mitigation plans can help ensure that the risk level is acceptable and the payroll process is secure and reliable. According to the CRISC Review Manual 2022, one of the key risk treatment techniques is to update the risk action plan, which is a document that outlines the risk mitigation plans1. According to the CRISC Review Questions, Answers & Explanations Manual 2022, updating the risk mitigation plans is the correct answer to this question2.
Payroll system risk factors, payroll process owner, and payroll administrative controls are not the first part of the risk register that should be updated when a migration is affecting a key risk scenario. Payroll system risk factors are the sources or causes of risk, such as threats, vulnerabilities, or uncertainties. Payroll process owner is the person who is responsible for the payroll process and its outcomes. Payroll administrative controls are the policies, procedures, or guidelines that govern the payroll process. These parts of the risk register may also need to be updated, but they are not as urgent or critical as the risk mitigation plans. Updating the risk factors, process owner, and administrative controls can help identify, assess, and monitor the risk, but they do not directly address the risk response. The risk response is the most important part of the risk management process, as it determines how the risk is handled and controlled.

NEW QUESTION: 733
When creating policies for a global organization with operations in multiple countries, which approach ensures compliance while addressing local regulations?
A. Develop policies with less restrictive requirements to ensure consistency across the organization.
B. Develop a global policy to be applied uniformly by each country.
C. Develop country-specific policies to address local regulations.

D. Develop a global policy that accommodates country-specific requirements.

Answer: (SHOW ANSWER)

A global policy that accommodates country-specific requirements balances consistency and compliance. It establishes a baseline of controls while allowing adaptation to local laws and cultural differences. Uniform application without adaptation risks non-compliance. Country-specific policies alone may lack global coherence. Therefore, accommodating local requirements within a global policy framework is best practice.

NEW QUESTION: 734

Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?

A. Risk tolerance is decreased.

B. Residual risk is increased.

C. Inherent risk is increased.

D. Risk appetite is decreased

Answer: (SHOW ANSWER)

A critical patch is a software update that fixes a security vulnerability or a bug that may affect the performance, functionality, or reliability of a system or a network. A critical patch implementation is a process that applies the software update to the system or network in a timely and effective manner. The failure of a critical patch implementation is a situation where the software update is not applied or not applied correctly, which may expose the system or network to various threats, such as data theft, data corruption, data leakage, or denial of service. The failure of a critical patch implementation would be reflected in an organization's risk profile by increasing the residual risk. Residual risk is the risk that remains after the risk response, which means the risk that is not avoided, transferred, or mitigated by the existing controls or measures. The failure of a critical patch implementation would increase the residual risk, as it would reduce the effectiveness or efficiency of the existing controls or measures that are supposed to address the security vulnerability or the bug. The failure of a critical patch implementation would also increase the likelihood or impact of the potential threats, as well as the exposure or consequences of the system or network. The other options are not the correct changes that would be reflected in an organization's risk profile after the failure of a critical patch implementation, although they may be affected or related. Risk tolerance is the degree of variation from the risk appetite that the organization is not willing to accept. Risk tolerance may be decreased by the failure of a critical patch implementation, as the organization may become more cautious or conservative in accepting the risk, but it is not a direct or immediate change in the risk profile. Inherent risk is the risk that exists in the absence of any controls or measures, which means the risk that is inherent to the system or network or the environment. Inherent risk may be increased by the failure of a critical patch implementation, as the system or network may become more vulnerable or susceptible to the threats, but it is not a change in the risk profile, as the risk profile considers the existing controls or measures. Risk appetite is the amount and type of risk that the organization is willing to accept in pursuit of its objectives. Risk appetite may be decreased by the failure of a critical patch implementation, as the organization may become less willing or able to accept the risk, but it is not a change in the risk profile, as the risk profile reflects the actual or current risk level, not the desired or expected risk level. References = CRISC Review Manual, pages 32-

331; CRISC Review Questions, Answers & Explanations Manual, page 972; What is a Critical Patch? - Definition from Techopedia3; What is Residual Risk? - Definition from Techopedia4

NEW QUESTION: 735
Which of the following would BEST provide early warning of a high-risk condition?
A. Risk register
B. Risk assessment
C. Key risk indicator (KRI)
D. Key performance indicator (KPI)
Answer: (SHOW ANSWER)
A key risk indicator (KRI) is a metric that provides information on the level of exposure to a given risk or the potential impact of a risk. KRIs are used to monitor changes in risk levels and alert management when a risk exceeds a predefined threshold or tolerance. KRIs can help provide early warning of a high-risk condition and enable timely response and mitigation actions. A risk register is a tool that records and tracks the identified risks, their likelihood, impact, and status. A risk assessment is a process that identifies, analyzes, and evaluates risks. A key performance indicator (KPI) is a metric that measures the achievement of a specific goal or objective. References = Risk IT Framework, pages 22-231; CRISC Review Manual, pages 44-452

NEW QUESTION: 736
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?
A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.
Answer: (SHOW ANSWER)
A risk practitioner's best course of action when a business manager wants to leverage an existing approved vendor solution from another area within the organization is to assess the risk associated with the new use case. This is because the new use case may introduce different or additional risks that were not considered or addressed in the original approval. For example, the new use case may involve different data types, volumes, or sensitivities; different business processes, functions, or objectives; different regulatory or contractual requirements; or different technical or operational dependencies. Therefore, the risk practitioner should perform a vendor risk assessment (VRA) to identify, evaluate, and mitigate the potential risks of the new use case and ensure that the vendor solution meets the organization's risk appetite and tolerance12. Recommending allowing the new usage based on prior approval is not the best course of action, as it may overlook or underestimate the risks of the new use case and expose the organization to unacceptable levels of risk. Requesting a new third-party review is not the best course of action, as it may be unnecessary or redundant if the vendor solution has already been reviewed and approved for another use case within the organization. Requesting revalidation of the original use case is not the best course of action, as it may not address the specific risks of the new use case and may also delay or disrupt the existing use case.

References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Risk Monitoring, pp. 189-191.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 737
Which of the following BEST reduces the probability of laptop theft?
A. Cable lock
B. Acceptable use policy
C. Data encryption
D. Asset tag with GPS
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, a cable lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a wall, to prevent unauthorized removal or theft. A cable lock is the best option to reduce the probability of laptop theft, as it acts as a deterrent and a barrier for potential thieves. A cable lock also helps to protect the confidentiality, integrity, and availability of the data stored on the laptop, as well as the laptop itself. References = CRISC Review Manual1, page 253.

NEW QUESTION: 738
Which of the following is a PRIMARY reason for considering existing controls during initial risk assessment?
A. To determine the inherent risk level
B. To determine the acceptable risk level
C. To determine the current risk level
D. To determine the desired risk level
Answer: (SHOW ANSWER)
During an initial risk assessment, it is crucial to consider existing controls primarily to determine the current risk level. Here's a Understanding Existing Controls:
Existing controls are measures already in place to mitigate risks. These controls can include technical, administrative, and physical safeguards designed to protect organizational assets.
Knowing what controls are currently in place helps to understand the organization's current defense mechanisms against potential threats.
Assessing the Current Risk Level:
The current risk level is the risk that remains after considering the effectiveness of existing controls, often referred to as residual risk.

By evaluating these controls, one can determine how much risk is actually mitigated and what level of risk remains.
For instance, if an organization has implemented firewalls and intrusion detection systems, these controls would reduce the risk of cyber attacks. The effectiveness of these controls will determine the residual risk level.
Differentiating Between Risk Types:
Inherent Risk:This is the level of risk that exists before any controls are applied. It's the raw risk associated with a particular asset or process.
Residual Risk:This is the risk that remains after existing controls have been applied. It's the actual risk that an organization faces after mitigation efforts.
Current Risk:This term is often used interchangeably with residual risk but focuses on the risk level at the present moment, considering the existing controls.
Primary Objective in Initial Risk Assessment:
The primary objective of considering existing controls during the initial risk assessment is to gain an accurate picture of the current risk landscape. This allows risk practitioners to understandwhat additional controls or modifications might be needed to further reduce risk to acceptable levels.
Without considering existing controls, the assessment would only reflect the inherent risk, which doesn't provide a realistic view of the organization's risk exposure.
References:
The CRISC Review Manual emphasizes the importance of understanding the current risk level by assessing existing controls (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.9.3 Current Risk).

NEW QUESTION: 739
Which of the following BEST supports the communication of risk assessment results to stakeholders?
A. Monitoring of high-risk areas
B. Classification of risk profiles
C. Periodic review of the risk register
D. Assignment of risk ownership
Answer: (SHOW ANSWER)
A risk profile is a summary of the key risks that affect an organization, a business unit, a process, or a project. A risk profile can help stakeholders understand the current and potential exposure to various sources of uncertainty, and prioritize the risk response accordingly. Classification of risk profiles is the process of grouping and categorizing risks based on common characteristics, such as source, impact, likelihood, or response strategy. Classification of risk profiles can help communicate risk assessment results to stakeholders by providing a clear and consistent way of presenting and comparing risks across different domains, levels, or perspectives. Classification of risk profiles can also help identify patterns, trends, and interrelationships among risks, and facilitate the allocation of resources and responsibilities for risk management. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.1: Risk Profile, p. 193-195.

NEW QUESTION: 740

Which of the following would MOST likely cause management to unknowingly accept excessive risk?

A. Satisfactory audit results

B. Risk tolerance being set too low

C. Inaccurate risk ratings

D. Lack of preventive controls

Answer: C (LEAVE A REPLY)

Inaccurate risk ratings would most likely cause management to unknowingly accept excessive risk, as they may not reflect the true level of risk exposure and impact, and may lead to inappropriate risk responses or decisions. Satisfactory audit results, risk tolerance being set too low, and lack of preventive controls are not the most likely causes, as they may indicate a different risk management issue, such as over-reliance on audit assurance, misalignment of risk tolerance and appetite, or insufficient risk mitigation, respectively.
References = CRISC Review Manual, 7th Edition, page 109.

NEW QUESTION: 741

As part of its risk strategy, an organization decided to transition its financial system from a cloud-based provider to an internally managed system. Which of the following should the risk practitioner do FIRST?

A. Reassess whether the risk responses properly address known risks and vulnerabilities

B. Analyze the risk register to identify potential updates and changes

C. Evaluate existing control test plans of the system for potential changes

D. Update the processes within impacted financial control assessments

Answer: (SHOW ANSWER)

Whenever there is a change in sourcing strategy, such as moving from cloud to internal hosting, the first step is to reassess the effectiveness and completeness of existing risk responses and confirm that they still mitigate the risks appropriately.
CRISC emphasizes:
"When transitioning services or changing control environments, practitioners should reassess risk responses and validate that previously identified risks and vulnerabilities remain properly addressed." Only after reassessment should the practitioner proceed to update registers, controls, and audit plans.
Hence, A is the correct answer.
CRISC Reference: Domain 3 - Risk Response and Mitigation, Topic: Managing Control Changes.

NEW QUESTION: 742

What is the GREATEST concern with maintaining decentralized risk registers instead of a consolidated risk register?

A. Aggregated risk may exceed the enterprise's risk appetite and tolerance.

B. Duplicate resources may be used to manage risk registers.

C. Standardization of risk management practices may be difficult to enforce.

D. Risk analysis may be inconsistent due to non-uniform impact and likelihood scales.

Answer: (SHOW ANSWER)

A risk register is a tool that records and tracks the identified risks, their causes, impacts, likelihood, responses, and owners. A decentralized risk register is maintained by each business unit or function, while a

consolidated risk register is maintained at the enterprise level. The greatest concern with maintaining decentralized risk registers instead of a consolidated risk register is that the aggregated risk may exceed the enterprise's risk appetite and tolerance. Risk appetite is the amount and type of risk that an enterprise is willing to accept in pursuit of its objectives, while risk tolerance is the acceptable level of variation around the objectives. If the risk registers are not consolidated, the enterprise may not have a holistic view of its risk profile and may not be able to prioritize and allocate resources effectively. The other options are also concerns, but they are not as significant as the potential misalignment between the aggregated risk and the enterprise's risk appetite and tolerance. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section
1.2.2.2, pp. 21-22.

NEW QUESTION: 743
Which of the following should be the FIRST consideration when establishing a new risk governance program?
A. Developing an ongoing awareness and training program
B. Creating policies and standards that are easy to comprehend
C. Embedding risk management into the organization
D. Completing annual risk assessments on critical resources
Answer: (SHOW ANSWER)
The first consideration when establishing a new risk governance program is embedding risk management into the organization. Embedding risk management means integrating risk management principles and practices into the organization's culture, values, processes, and decision-making. Embedding risk management helps to ensure that risk management is not seen as a separate or isolated activity, but as a part of the organization's normal operations and strategic objectives. Embedding risk management also helps to create a risk-aware and risk-responsive organization, where risk management is shared and supported by all stakeholders. The other options are not the first consideration, although they may be important steps or components of the risk governance program. Developing an ongoing awareness and training program, creating policies and standards that are easy to comprehend, and completing annual risk assessments on critical resources are all activities that can help to embed risk management into the organization, but they are not the initial or primary consideration. References = Risk and Information Systems Control Study Manual, Chapter 1, Section 1.2.1, page 1-8.

NEW QUESTION: 744
An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?
A. Data may be commingled with other tenants' data.
B. System downtime does not meet the organization's thresholds.
C. The infrastructure will be managed by the public cloud administrator.
D. The cloud provider is not independently certified.
Answer: (SHOW ANSWER)

The greatest security risk in this scenario is that data may be commingled with other tenants' data on the public cloud infrastructure. Data commingling occurs when data from different sources or customers are mixed together without proper segregation or encryption. This may result in data leakage, unauthorized access, or loss of confidentiality and integrity. Data commingling is a common challenge in public cloud environments, where multiple customers share the same physical resources and network. System downtime, infrastructure management, and cloud provider certification are also potential risks in this scenario, but they are not as great as data commingling. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.2.1.1, page 2451
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 638.

NEW QUESTION: 745
Which of the following MUST be assessed before considering risk treatment options for a scenario with significant impact?
A. Risk magnitude
B. Incident probability
C. Risk appetite
D. Cost-benefit analysis
Answer: (SHOW ANSWER)
According to the Risk Assessment and Management: A Complete Guide, risk magnitude is the product of the likelihood and impact of a risk scenario. Risk magnitude is an important factor to consider before choosing risk treatment options, as it indicates the level of exposure and potential harm that the organization faces from the risk scenario. Risk treatment options should be selected based on the risk magnitude, as well as the risk appetite and tolerance of the organization. For a scenario with significant impact, the risk magnitude is likely to be high, and therefore the risk treatment options should aim to reduce the likelihood and/or impact of the risk scenario as much as possible, or to transfer or avoid the risk altogether. References = Risk Assessment and Management: A Complete Guide, ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide

NEW QUESTION: 746
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?
A. Enhance the security awareness program.
B. Increase the frequency of incident reporting.
C. Purchase cyber insurance from a third party.
D. Conduct a control assessment.
Answer: (SHOW ANSWER)
A control assessment is the process of evaluating the design and effectiveness of controls that are implemented to mitigate risks. A control assessment can help identify the root causes of data loss, thegaps in the existing controls, and the potential solutions to improve the control environment. A control assessment should be conducted after identifying a high probability of data loss in a system, as it can provide valuable

information for risk response and reporting. References = Risk and Information Systems Control Study Manual, Chapter 3: Risk Response and Mitigation, Section 3.2: Control Assessment, p. 147-149.

NEW QUESTION: 747
Which of the following is the MOST important update for keeping the risk register current?
A. Modifying organizational structures when lines of business merge
B. Adding new risk assessment results annually
C. Retiring risk scenarios that have been avoided
D. Changing risk owners due to employee turnover
Answer: A (LEAVE A REPLY)
Understanding the Question:
The question asks what the most important update for keeping the risk register current is.
Analyzing the Options:
A). Modifying organizational structures when lines of business merge:Reflects significant changes in the organization that impact risk profiles.
B). Adding new risk assessment results annually:Important but periodic.
C). Retiring risk scenarios that have been avoided:Necessary but not as impactful as major organizational changes.
D). Changing risk owners due to employee turnover:Important but secondary to major structural changes.
Organizational Changes:When lines of business merge, it can significantly alter the risk landscape, introducing new risks and changing the impact and likelihood of existing ones. Updating the risk register to reflect these changes is crucial for accurate risk management.
Impact on Risk Profiles:Mergers and acquisitions can affect every aspect of an organization, from operational processes to regulatory compliance, making it essential to update the risk register accordingly.
References:
CRISC Review Manual, Chapter 3: Risk Response and Reporting, discusses the importance of keeping the risk register updated to reflect organizational changes and ensure effective risk management.

NEW QUESTION: 748
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?
A. Senior management has approved the control design.
B. Inherent risk has been reduced from original levels.
C. Residual risk remains within acceptable levels.
D. Costs for control maintenance are reasonable.
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after the implementation of controls. It is important for a risk practitioner to verify that the residual risk is within the acceptable levels defined by the enterprise's risk appetite and tolerance. This ensures that the controls are effective in reducing the risk exposure to an acceptable level and align with the enterprise's objectives and strategy. References = CRISC Review Manual 27th Edition, page

131. Most Asked CRISC Exam Questions and Answers.

NEW QUESTION: 749
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"
A. A summary of risk response plans with validation results
B. A report with control environment assessment results
C. A dashboard summarizing key risk indicators (KRIs)
D. A summary of IT risk scenarios with business cases
Answer: (SHOW ANSWER)
A dashboard summarizing key risk indicators (KRIs) is the best way for a risk practitioner to present an annual risk management update to the board because it provides a concise and visual overview of the current risk status, trends, and performance of the organization. KRIs are metrics that measure the likelihood and impact of risks, and help the board monitor and prioritize the most critical risks. A summary of risk response plans, a report with control environment assessment results, and a summary of IT risk scenarios are all useful information, but they are too detailed and technical for the board, who needs a high-level and strategic view of the risk management program. References = Risk and Information Systems Control Study Manual, Chapter
4, Section 4.4.1, page 4-36.

NEW QUESTION: 750
A poster has been displayed in a data center that reads. "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?
Freecram.net
A. Corrective
B. Detective
C. Deterrent
D. Preventative
Answer: (SHOW ANSWER)
A deterrent control is a type of control that has been implemented by displaying a poster that reads "Anyone caught taking photographs in the data center may be subject to disciplinary action.", as it aims to discourage or prevent unauthorized or malicious activities by warning the potential perpetrators of the consequences or sanctions. The other options are not the correct types of control, as they are more related to the correction, detection, or prevention of unauthorized or malicious activities, respectively, rather than the deterrence of unauthorized or malicious activities. References = CRISC Review Manual, 7th Edition, page 154.

NEW QUESTION: 751
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?
A. Identify previous data breaches using the startup company's audit reports.

B. Have the data privacy officer review the startup company's data protection policies.
C. Classify and protect the data according to the parent company's internal standards.
D. Implement a firewall and isolate the environment from the parent company's network.
Answer: (SHOW ANSWER)
Data protection is the process of safeguarding sensitive personal information from unauthorized access, use, disclosure, modification, or destruction. Data protection can help to ensure the privacy and security ofthe data subjects, and to comply with the legal and regulatory requirements that apply to the data processing activities1.
A highly regulated organization that acquired a medical technology startup company that processes sensitive personal information with weak data protection controls faces a high risk of data breaches, fines, lawsuits, reputational damage, or loss of customer trust. The best way for the acquiring company to reduce its risk while still enabling the flexibility needed by the startup company is to classify and protect the data according to the parent company's internal standards, because it can help to:
Identify and categorize the sensitive personal information based on its value, sensitivity, and criticality, such as confidential, restricted, internal, or public Apply and enforce the appropriate data protection policies, procedures, and controls for each data category, such as encryption, access control, backup, retention, or disposal Align and integrate the data protection practices and processes of the startup company with those of the parent company, and ensure the consistency and compliance across the organization Balance and optimize the trade-off between data protection and data usability, and allow the startup company to leverage the data for innovation and growth, as long as it meets the data protection standards of the parent company23 The other options are not the best ways for the acquiring company to reduce its risk while still enabling the flexibility needed by the startup company, but rather some of the steps or aspects of data protection. Identify previous data breaches using the startup company's audit reports is a step that can help to assess the current data protection status and gaps of the startup company, and to learn from the past incidents and mistakes, but it does not address the future data protection needs and challenges of the startup company. Have the data privacy officer review the startup company's data protection policies is an aspect that can help to ensure the legal and regulatory compliance of the data protection activities of the startup company, and to provide guidance and oversight for the data protection issues and risks, but it does not ensure the technical and operational effectiveness and efficiency of the data protection controls of the startup company. Implement a firewall and isolate the environment from the parent company's network is a control that can help to prevent or limit the external or internal attacks or threats to the data of the startup company, and to reduce the exposure or impact of a data breach, but it does not ensure the availability or accessibility of the data for the legitimate and authorized purposes of the startup company. References = Data Protection - ISACA Data Classification - ISACA Data Protection Best Practices - ISACA
[CRISC Review Manual, 7th Edition]

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here:

https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 752
Who is the BEST person to an application system used to process employee personal data?
A. Compliance manager
B. Data privacy manager
C. System administrator
D. Human resources (HR) manager
Answer: (SHOW ANSWER)
The data privacy manager is the best person to an application system used to process employee personal data, because they are responsible for ensuring that the organization complies with the applicable data protection laws and regulations, and that the personal data of employees are collected, stored, processed, and disposed of in a secure and ethical manner. The data privacy manager is also responsible for establishing and maintaining the data privacy policies, procedures, and controls, and for conducting data privacy impact assessments and audits. The compliance manager, the system administrator, and the human resources (HR) manager are all involved in the of the application system, but they are not the best person to it, as they do not have the primary accountability and expertise for data privacy. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

NEW QUESTION: 753
A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees. Which of the following is the risk practitioner's BEST course of action?
A. Contact the control owner to determine if a gap in controls exists.
B. Add this concern to the risk register and highlight it for management review.
C. Report this concern to the contracts department for further action.
D. Document this concern as a threat and conduct an impact analysis.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, the contracts department is responsible for drafting, reviewing, and negotiating contracts with vendors and other third parties. The contracts department should ensure that the contracts include adequate clauses and terms to address the risks and controls related to the vendor services and activities. Therefore, the best course of action for the risk practitioner when finding a missing clause to control privileged access to the organization's systems by vendor employees is to report this concern to the contracts department for further action. The contracts department can then revise the contract to include the necessary clause, or seek alternative solutions to mitigate the risk of unauthorized or inappropriate access by vendor employees. References = CRISC Review Manual1, page 229.

NEW QUESTION: 754
If concurrent update transactions to an account are not processed properly, which of the following will MOST likely be affected?

A. Confidentiality
B. Accountability
C. Availability
D. Integrity
Answer: (SHOW ANSWER)
Integrity is the property of data that ensures its accuracy, completeness, and consistency2. If concurrent update transactions to an account are not processed properly, the integrity of the data may be compromised, as it may lead to concurrency problems such as lost update, unrepeatable read, or phantom read3. These problems can cause the data to be incorrect, incomplete, or inconsistent, which may affect the reliability and validity of the data. Therefore, option D is the correct answer, as it reflects the impact of improper concurrent update transactions on the data integrity. The other options are not correct, as they do not directly relate to the effect of concurrent update transactions on the data. Option A, confidentiality, is the property of data that ensures its protection from unauthorized access or disclosure2. Concurrent update transactions do not necessarily affect the confidentiality of the data, as they do not involve exposing the data to unauthorized parties. Option B, accountability, is the property of data that ensures its traceability and auditability2. Concurrent update transactions do not necessarily affect the accountability of the data, as they do not involve losing the records or logs of the data transactions. Option C, availability, is the property of data that ensures its accessibility and usability2. Concurrent update transactions do not necessarily affect the availability of the data, as they do not involve preventing the access or use of the data.

NEW QUESTION: 755
Which of the following is the BEST way to address a board's concern about the organization's current cybersecurity posture?
A. Assess security capabilities against an industry framework
B. Create a new security risk officer role.
C. Increase the frequency of vulnerability testing.
D. Update security risk scenarios.
Answer: (SHOW ANSWER)

NEW QUESTION: 756
An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?
A. Reassess whether mitigating controls address the known risk in the processes.
B. Update processes to address the new technology.
C. Update the data governance policy to address the new technology.
D. Perform a gap analysis of the impacted processes.
Answer: (SHOW ANSWER)
Robotic process automation (RPA) is the use of software robots or artificial intelligence (AI) agents to automate repetitive, rule-based tasks that are normally performed by humans. RPA can improve efficiency, accuracy, and scalability of business processes, but it can also introduce new risks or change the existing

risk profile. Therefore, the risk practitioner's best course of action is to reassess whether the mitigating controls that were designed for the human-performed processes are still effective and adequate for the RPA-enabled processes. This may involve reviewing the control objectives, testing the control performance, identifying the control gaps, and recommending the control enhancements or modifications. References = CRISC Review Manual, 7th Edition, page 177.

NEW QUESTION: 757
The MOST effective way to increase the likelihood that risk responses will be implemented is to:
A. create an action plan
B. assign ownership
C. review progress reports
D. perform regular audits.
Answer: B (LEAVE A REPLY)
* Risk responses are the actions or strategies that are taken to address the risks that may affect the organization's objectives, performance, or value creation12.
* The most effective way to increase the likelihood that risk responses will be implemented is to assign ownership, which is the process of identifying and appointing the individuals or groups who are responsible and accountable for the execution and monitoring of the risk responses34.
* Assigning ownership is the most effective way because it ensures the clarity and commitment of the roles and responsibilities for the risk responses, and avoids the confusion or ambiguity that may arise from the lack of ownership34.
* Assigning ownership is also the most effective way because it enhances the communication and collaboration among the stakeholders involved in the risk responses, and provides the feedback and input that are necessary for the improvement and optimization of the risk responses34.
* The other options are not the most effective way, but rather possible steps or tools that may support or complement the assignment of ownership. For example:
* Creating an action plan is a step that involves defining and documenting the specific tasks, resources, timelines, and deliverables for the risk responses34. However, this step is not the most effective way because it does not guarantee the implementation of the risk responses, especially if there is no clear or agreed ownership for the action plan34.
* Reviewing progress reports is a tool that involves collecting and analyzing the information and data on the status and performance of the risk responses, and identifying the issues or gaps that need to be addressed34. However, this tool is not the most effective way because it does not ensure the implementation of the risk responses, especially if there is no ownership for the progress reports or the corrective actions34.
* Performing regular audits is a tool that involves conducting an independent and objective assessment of the adequacy and effectiveness of the risk responses, and providing the findings and recommendations for improvement56. However, this tool is not the most effective way because it does not ensure the implementation of the risk responses, especially if there is no ownership for the audit results or the follow-up actions56. References =
* 1: Risk IT Framework, ISACA, 2009
* 2: IT Risk Management Framework, University of Toronto, 2017

* 3: Risk Response Plan in Project Management: Key Strategies & Tips1
* 4: ProjectManagement.com - How to Implement Risk Responses2
* 5: IT Audit and Assurance Standards, ISACA, 2014
* 6: IT Audit and Assurance Guidelines, ISACA, 2014

NEW QUESTION: 758
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?
A. Management approval
B. Annual review
C. Relevance
D. Automation
Answer: (SHOW ANSWER)
The most important factor to the effectiveness of key performance indicators (KPIs) is relevance. KPIs are metrics that measure the achievement of the objectives or the performance of the processes. Relevance means that the KPIs are aligned with and support the strategic goals and priorities of the organization, and that they reflect the current and desired state of the outcomes or outputs. Relevance also means that the KPIs are meaningful and useful for the decision makers and stakeholders, and that they provide clear and actionable information for improvement or optimization. The other options are not as important as relevance, as they are related to the approval, review, or automation of the KPIs, not the quality or value of the KPIs. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Key Performance Indicators, page 183.

NEW QUESTION: 759
The PRIMARY goal of a risk management program is to:
A. facilitate resource availability.
B. help ensure objectives are met.
C. safeguard corporate assets.
D. help prevent operational losses.
Answer: (SHOW ANSWER)
According to the What Is Risk Management & Why Is It Important? article, risk management is the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect your organization. The primary goal of a risk management program is to help ensure objectives are met, by aligning the risk management process with the organization's strategy, vision, mission, values, and objectives.
By having a risk management program, an organization can identify potential problems before they occur and have a plan for addressing them, as well as monitor and report on the effectiveness of the risk responses. This can help the organization to achieve its desired outcomes and create value for its stakeholders. References = What Is Risk Management & Why Is It Important?

NEW QUESTION: 760

A key performance indicator (KPI) shows that a process is operating inefficiently, even though no control issues were noted during the most recent risk assessment. Which of the following should be done FIRST?

Freecram.net

A. Implement new controls.
B. Recalibrate the key performance indicator (KPI).
C. Redesign the process.
D. Re-evaluate the existing control design.
Answer: (SHOW ANSWER)
Understanding KPIs:
Key Performance Indicators (KPIs) are metrics used to evaluate the efficiency and effectiveness of a process.
They must be accurate and relevant to provide meaningful insights.
Process Inefficiency Despite No Control Issues:
If a KPI shows inefficiency but no control issues are noted, it suggests that the KPI may not be accurately reflecting the process performance.
Recalibrating the KPI ensures that it correctly measures what it is intended to, providing a true picture of the process efficiency.
Steps for Recalibration:
Review the current KPI and its alignment with process objectives.
Adjust the KPI parameters or thresholds to better reflect process performance.
Validate the recalibrated KPI with historical data to ensure accuracy.
Comparing Other Actions:
Implementing New Controls:Premature without understanding the root cause of the KPI discrepancy.
Redesigning the Process:Extensive and unnecessary if the KPI is simply miscalibrated.
Re-Evaluating Existing Control Design:Important but secondary to ensuring KPI accuracy.
References:
The CRISC Review Manual emphasizes the importance of accurate KPIs in monitoring process performance and the need for recalibration when discrepancies are found (CRISC Review Manual, Chapter 3: Risk Response and Mitigation, Section 3.14 Key Performance Indicators).

NEW QUESTION: 761
Legal and regulatory risk associated with business conducted over the Internet is driven by:
A. the jurisdiction in which an organization has its principal headquarters
B. international law and a uniform set of regulations.
C. the laws and regulations of each individual country
D. international standard-setting bodies.
Answer: (SHOW ANSWER)
The legal and regulatory risk associated with business conducted over the Internet is driven by the laws and regulations of each individual country. Legal and regulatory risk is the risk of non-compliance or violation of the applicable laws and regulations that govern the business activities, operations, or transactions. Business conducted over the Internet involves the use of the global network of interconnected computers and devices

to exchange information, goods, or services across the geographic boundaries. Business conducted over the Internet may expose the enterprise to various legal and regulatory risks, such as data protection, privacy, security, intellectual property, consumer protection, taxation, or jurisdiction issues. The legal and regulatory risk associated with business conducted over the Internet is driven by the laws and regulations of each individual country, as each country may have different or conflicting laws and regulations that apply to the business conducted over the Internet, and that may change or vary over time. The laws and regulations of each individual country may also impose different or additional obligations, requirements, or restrictions on the enterprise, and may subject the enterprise to different or multiple enforcement actions, penalties, or disputes.
The jurisdiction in which an organization has its principal headquarters, international law and a uniform set of regulations, and international standard-setting bodies are not the drivers of the legal and regulatory risk associated with business conducted over the Internet, as they do not reflect the diversity and complexity of the legal and regulatory landscape that the enterprise may face when conducting business over the Internet. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 762
Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?
A. Establishing a risk management committee
B. Updating the organization's risk register to reflect the new threat
C. Communicating the results of the threat impact analysis
D. Establishing metrics to assess the effectiveness of the responses
Answer: (SHOW ANSWER)
According to the CRISC Review Manual1, threat impact analysis is the process of estimating and evaluating the potential effects of a threat event on the organization's objectives, processes, resources, and risks. Threat impact analysis helps to quantify and qualify the severity and likelihood of the threat, and to identify the possible consequences and implications for the organization. Communicating the results of the threat impact analysis is the most effective way to improve stakeholders' understanding of the effect of a potential threat, as it helps to inform and educate the stakeholders about the nature and magnitude of the threat, and to solicit their feedback and input for the risk response. Communicating the results of the threat impact analysis also helps to align the stakeholder expectations and preferences, and to facilitate risk-based decision making and action planning. References = CRISC Review Manual1, page 208.

NEW QUESTION: 763
A cote data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the to" owing would provide the MOST useful information to determine mitigating controls?
A. Forensic analysis
B. Risk assessment
C. Root cause analysis
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

The most useful information to determine mitigating controls when a core data center went offline abruptly for several hours affecting many transactions across multiple locations is the root cause analysis. Root cause analysis is a technique that identifies the underlying factors or reasons that caused the problem or incident. Root cause analysis can help to understand the nature, scope, and impact of the problem or incident, and to prevent or reduce the recurrence or severity of the problem or incident in the future. Root cause analysis can also help to identify and prioritize the appropriate mitigating controls that address the root causes of the problem or incident. The other options are not as useful as root cause analysis, as they are related to the investigation, evaluation, or measurement of the problem or incident, not the resolution or prevention of the problem or incident. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.4: Key Control Indicators, page 211.

NEW QUESTION: 764
The BEST indication that risk management is effective is when risk has been reduced to meet:
A. risk levels.
B. risk budgets.
C. risk appetite.
D. risk capacity.
Answer: (SHOW ANSWER)
The best indication that risk management is effective is when risk has been reduced to meet the risk appetite of the enterprise. Risk appetite is the amount and type of risk that an enterprise is willing to accept in pursuit of its objectives. Risk appetite reflects the enterprise's risk culture, strategy, and values, and provides a basis for setting risk tolerance levels and risk response strategies. Risk management is effective when it enables the enterprise to align its risk exposure with its risk appetite, and to optimize the risk-return trade- off. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.2.1, page 181

NEW QUESTION: 765
Which of the following is the MOST important outcome of a business impact analysis (BIA)?
A. Understanding and prioritization of critical processes
B. Completion of the business continuity plan (BCP)
C. Identification of regulatory consequences
D. Reduction of security and business continuity threats
Answer: (SHOW ANSWER)
The most important outcome of a business impact analysis (BIA) is understanding and prioritization of critical processes. A BIA is a process that identifies and evaluates the potential effects of disruptions or disasters on the organization's business functions and processes. A BIA helps to understand the dependencies, interrelationships, and impacts of the business processes, and to prioritize them based on their importance and urgency. A BIA also helps to determine the recovery objectives, strategies, and resources for the business processes, such as the recovery time objective (RTO), the recovery point objective (RPO), and the minimum operating requirements (MOR). The other options are not as important as understanding and prioritization of critical processes, although they may be part of or derived from the BIA. Completion of the

business continuity plan (BCP), identification of regulatory consequences, and reduction of security and business continuity threats are all activities or outcomes that can be supported or facilitated by the BIA, but they are not the primary purpose or result of the BIA. References = CISA Review Manual, 27th Edition, Chapter 5, Section 5.2.1, page 5-9.

NEW QUESTION: 766
The MOST important reason for implementing change control procedures is to ensure:
A. only approved changes are implemented
B. timely evaluation of change events
C. an audit trail exists.
D. that emergency changes are logged.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, the most important reason for implementing change control procedures is to ensure that only approved changes are implemented, because it helps to prevent or minimize the risk of unauthorized or unintended changes that may affect the stability, security, or performance of the IT systems and processes. Change control procedures are the steps and activities that are followed to manage the initiation, review, approval, implementation, and verification of changes. Change control procedures also help to ensure that the changes are aligned with the business requirements and objectives, and that the changes are documented and communicated to the stakeholders. The other options are not the most important reason for implementing change control procedures, as they are related to other benefits or outcomes of the change control process. Timely evaluation of change events is the reason for implementing change management, which is the process of identifying, analyzing, and responding to the changes that may affect the IT systems and processes. An audit trail is the outcome of implementing change control procedures, as it provides a record of the changes and their impacts. Logging emergency changes is the exception of implementing change control procedures, as it allows for bypassing the normal approval process in case of urgent or critical changes. References = CRISC Review Manual, 7th Edition, Chapter 4, Section 4.2.1, page 177.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 767
An organization recently experienced a cyber attack that resulted in the loss of confidential customer data. Which of the following is the risk practitioner's BEST recommendation after recovery steps have been completed?
A. Develop new key risk indicators (KRIs).

B. Perform a root cause analysis.
C. Recommend the purchase of cyber insurance.
D. Review the incident response plan.
Answer: (SHOW ANSWER)
The risk practitioner's best recommendation after recovery steps have been completed is B. Perform a root cause analysis. A root cause analysis is a process of identifying and assessing the underlying causes of a problem or an incident. By performing a root cause analysis, the risk practitioner can help the organization to understand how and why the cyber attack happened, what vulnerabilities and gaps were exploited, and what actions and controls can be implemented to prevent or mitigate similar incidents in the future12 A root cause analysis can also help the organization to improve its incident response plan, which is a set of instructions to help IT staff detect, respond to, and recover from network security incidents3 A root cause analysis can provide valuable feedback and lessons learned from the cyber attack, and help the organization to update and test its incident response plan accordingly45 Developing new key risk indicators, recommending the purchase of cyber insurance, and reviewing the incident response plan are all possible actions that the risk practitioner can take after a cyber attack, but they are not the best recommendation. Developing new key risk indicators can help the organization to monitor and measure its risk exposure and performance, but it does not address the root causes of the cyber attack12 Recommending the purchase of cyber insurance can help the organization to hedge against the financial losses caused by cyber incidents, but it does not prevent or solve the underlying issues67 Reviewing the incident response plan can help the organization to evaluate its effectiveness and identify areas for improvement, but it does not explain how and why the cyber attack occurred345 Therefore, the best recommendation is to perform a root cause analysis, as it can help the organization to understand, resolve, and prevent the cyber attack and its consequences12

NEW QUESTION: 768
Which of the following is the GREATEST risk associated with inappropriate classification of data?
A. Inaccurate record management data
B. Inaccurate recovery time objectives (RTOs)
C. Lack of accountability for data ownership
D. Users having unauthorized access to data
Answer: (SHOW ANSWER)
The greatest risk associated with inappropriate classification of data is users having unauthorized access to sensitive information. Proper data classification ensures that access controls are applied appropriately, protecting sensitive data from unauthorized access.
* Importance of Data Classification
* Data classification involves categorizing data based on its level of sensitivity and the impact that unauthorized access, disclosure, modification, or destruction would have on the organization.
* It ensures that appropriate security measures are applied according to the data's classification.
* Risks of Inappropriate Classification
* Unauthorized Access: If data is not classified correctly, sensitive information may not receive the necessary protections, leading to unauthorized access.

* Lack of Accountability: Misclassification can result in unclear responsibilities for data protection, but the primary concern remains unauthorized access.
* Inaccurate Recovery Time Objectives (RTOs): While important, this is secondary to the risk of unauthorized access.
* Inaccurate Record Management Data: This can affect operational efficiency but is not as critical as unauthorized access.
* Implementing Effective Classification
* Organizations must have a clear data classification policy and ensure it is followed consistently.
* Regular audits and reviews should be conducted to verify that data is classified appropriately and that access controls are enforced.
References
* CISM Review Manual Full text.html, emphasizing the importance of proper data classification and the risks associated with misclassification, especially unauthorized access to data.

NEW QUESTION: 769
Which of the following is the PRIMARY benefit of using a risk map with stakeholders?
A. Consolidates risk response options by severity
B. Aligns risk appetite with business objectives
C. Correlates risk scenarios to risk appetite
D. Defines an organizational risk taxonomy
Answer: (SHOW ANSWER)
Arisk maphelps stakeholders understand how risk scenarios align with the organization'srisk appetite. This visualization facilitates informed decision-making and ensures risk responses are consistent with organizational priorities.

NEW QUESTION: 770
An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?
freecram.net
A. Secure encryption protocols are utilized.
B. Multi-factor authentication is set up for users.
C. The solution architecture is approved by IT.
D. A risk transfer clause is included in the contact
Answer: (SHOW ANSWER)
Utilizing secure encryption protocols is the most important factor to mitigate risk associated with data privacy when implementing a new Software as a Service (SaaS) speech-to-text solution, as it ensures that the data is protected from unauthorized access, interception, or modification during the transmission and storage in the cloud. Setting up multi-factor authentication for users, approving the solution architecture by IT, and including a risk transfer clause in the contract are not the most important factors, as they may not address the data privacy issue, but rather the data access, quality, or liability issue, respectively. References = CRISC Review Manual, 7th Edition, page 153.

NEW QUESTION: 771
Which of the following would cause the GREATEST concern for a risk practitioner reviewing the IT risk scenarios recorded in an organization's IT risk register?
A. Some IT risk scenarios have multi-year risk action plans.
B. Several IT risk scenarios are missing assigned owners.
C. Numerous IT risk scenarios have been granted risk acceptances.
D. Many IT risk scenarios are categorized as avoided.
Answer: (SHOW ANSWER)
Assigning ownership to each risk scenario is fundamental in risk management. Without designated owners, there is a lack of accountability, which can lead to risks not being adequately managed or mitigated. The absence of assigned owners means that no one is responsible for monitoring, reporting, or addressing the risk, increasing the likelihood of adverse outcomes.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 2: IT Risk Assessment, Section: Risk Ownership.

NEW QUESTION: 772
Which of the following is the BEST method for determining an enterprise's current appetite for risk?
A. Comparative analysis of peer companies
B. Reviews of brokerage firm assessments
C. Interviews with senior management
D. Trend analysis using prior annual reports
Answer: (SHOW ANSWER)
Conducting interviews with senior management is the best method for determining an enterprise's current appetite for risk, because it helps to obtain the direct and qualitative input and feedback from the senior management on their expectations and preferences regarding the level and type of risk that the enterprise is willing to accept or pursue, in relation to its objectives and strategy. Risk appetite is the amount and nature of risk that an enterprise is willing to take in order to achieve its objectives and create value. Risk appetite is influenced by factors such as the enterprise's culture, values, vision, mission, and strategy, as well as the external environment and stakeholders. Risk appetite may vary depending on the context and situation, and may change over time. Conducting interviews with senior management is the best method, as it helps to understand and capture the current and explicit risk appetite of the enterprise, and to align the risk management process and activities with the senior management's risk vision and direction. Conducting comparative analysis of peer companies, reviewing brokerage firm assessments, and performing trend analysis using prior annual reports are all possible methods for determining an enterprise's current appetite for risk, but they are not the best method, as they may provide only indirect, quantitative, or historical information, and may not reflect the current and specific risk appetite of the enterprise. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.1, page 45

NEW QUESTION: 773

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?

A. Temporarily suspend emergency changes.

B. Document the control deficiency in the risk register.

C. Conduct a root cause analysis.

D. Continue monitoring change management metrics.

Answer: (SHOW ANSWER)

According to the CRISC Review Manual, a root cause analysis is a technique that identifies the underlying causes of an event or a problem. It helps to determine the most effective actions to prevent or mitigate the recurrence of the event or problem. A root cause analysis is the best approach for the risk practitioner to take in this scenario, because it will help to understand why the number of emergency changes has increased substantially and what can be done to address the issue. The other options are not the best approaches, because they do not address the underlying causes of the problem. Temporarily suspending emergency changes may disrupt the business operations and create more risks. Documenting the control deficiency in the risk register is a passive action that does not resolve the problem. Continuing monitoring change management metrics is an ongoing activity that does not provide any insight into the problem. References = CRISC Review Manual, 7th Edition, Chapter 3, Section 3.2.4, page 130.

NEW QUESTION: 774

A chief risk officer (CRO) has asked to have the IT risk register integrated into the enterprise risk management (ERM) process. Which of the following will BEST facilitate the reporting of IT risk at the enterprise level?

A. Aggregating the IT risk scenarios into a maturity benchmark value

B. Using an IT risk heat map to depict likelihood and impact

C. Using the same risk taxonomy across the organization

D. Providing a summary of open IT risk-related audit findings

Answer: (SHOW ANSWER)

Using aconsistent risk taxonomyensures that IT risks can be aggregated and compared with enterprise-level risks in a meaningful way. ISACA emphasizes that standardized risk language and categories are critical to integrating IT risk with ERM processes.

NEW QUESTION: 775

Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

A. An acceptable use policy for personal devices

B. Required user log-on before synchronizing data

C. Enforced authentication and data encryption

D. Security awareness training and testing

Answer: C (LEAVE A REPLY)

The risk associated with the loss of company data stored on personal devices is that the data may be accessed, disclosed, or modified by unauthorized parties, resulting in confidentiality, integrity, or availability breaches1.
The most effective way to mitigate this risk is to enforce authentication and data encryption on the personal devices that store company data. Authentication is a process that verifies the identity of the user or device that is accessing the data, and prevents unauthorized access by requiring a password, a code, a biometric factor, or a combination of these2. Data encryption is a technique that transforms the data into an unreadable format, and requires a key to decrypt and restore the data to its original format3. By enforcing authentication and data encryption on the personal devices, the organization can ensure that only authorized users or devices can access the company data, and that the data is protected from unauthorized disclosure or modification even if the device is lost or stolen4. An acceptable use policy for personal devices, required user log-on before synchronizing data, and security awareness training and testing are not the most effective ways to mitigate the risk associated with the loss of company data stored on personal devices, as they do not provide the same level of protection as authentication and data encryption. An acceptable use policy for personal devices is a document that defines the rules and guidelines for using personal devices for work purposes, such as the types of devices, data, and applications that are allowed, the security measures that are required, and the responsibilities and liabilities of the users and the organization5. An acceptable use policy for personal devices can help to establish a common understanding and expectation for the use of personal devices, but it does not enforce or guarantee the compliance or effectiveness of the security measures. Required user log-on before synchronizing data is a technique that requires the user to enter their credentials before they can transfer or update the data between their personal device and the company network or system6. Required user log-on before synchronizing data can help to prevent unauthorized synchronization of data, but it does not protect the data that is already stored on the personal device. Security awareness training and testing is a process that educates and evaluates the users on the security risks and best practices for using personal devices for work purposes, such as the importance of using strong passwords, updating software, avoiding phishing emails, and reporting incidents7. Security awareness training and testing can help to increase the knowledge and behavior of the users, but it does not ensure or monitor the implementation or performance of the security measures. References = 1: BYOD security: What are the risks and how can they be mitigated?
2: What is Multi-Factor Authentication (MFA)? | Duo Security3: [What is Data Encryption? | Definition and FAQs] 4: How to mitigate the risks of using personal devices in the workplace5: BYOD Policy Template - Get Free Sample6: How to Sync Your Phone With Windows 10 | PCMag7: Security Awareness Training: What Is It and Why Is It Important?

NEW QUESTION: 776
An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?
A. Disaster recovery plan (DRP) of the system
B. Right to audit the provider
C. Internal controls to ensure data privacy
D. Transparency of key performance indicators (KPIs)

Answer: C (LEAVE A REPLY)

The most important consideration when selecting an external service provider for outsourcing the payroll function is the internal controls to ensure data privacy. The payroll function involves processing and storingsensitive personal and financial information of the employees, such as salaries, taxes, benefits, bank accounts, etc. This information needs to be protected from unauthorized access, disclosure, modification, or loss, as it may result in legal, regulatory, reputational, or financial consequences for the organization and the employees. Therefore, the external service provider should have adequate internal controls, such as encryption, access control, backup, logging, monitoring, etc., to ensure data privacy and compliance with the organization's policies and standards. Disaster recovery plan, right to audit, and transparency of KPIs are also important considerations when selecting an external service provider, but they are not as important as internal controls to ensure data privacy. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.2.1.2, page 2461

1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 648.

NEW QUESTION: 777

Which of the following is MOST important when developing key risk indicators (KRIs)?

A. Alignment with regulatory requirements

B. Availability of qualitative data

C. Properly set thresholds

D. Alignment with industry benchmarks

Answer: (SHOW ANSWER)

The most important factor when developing key risk indicators (KRIs) is to properly set thresholds, which are the predefined values or ranges that indicate the acceptable or unacceptable level of risk1. Thresholds can help to:

Trigger alerts or actions when the risk level exceeds or falls below the threshold, and enable timely and appropriate risk responses2.

Measure and monitor the performance and effectiveness of the risk responses, and ensure that the residual risk is within the risk appetite and tolerance3.

Communicate and report the risk status and performance to the stakeholders, and facilitate the decision-making and accountability for the risk management4.

The other factors are not the most important when developing KRIs, because:

Alignment with regulatory requirements is a necessary but not sufficient factor when developing KRIs, as it ensures that the KRIs comply with the applicable laws, rules, or standards that govern the organization's activities and operations5. However, alignment with regulatory requirements does not guarantee that the KRIs are relevant and useful for the organization's specific risk profile and objectives.

Availability of qualitative data is a desirable but not essential factor when developing KRIs, as it provides additional information or insights that may not be captured by quantitative data, such as opinions, perceptions, or feedback. However, availability of qualitative data does not ensure that the KRIs are reliable and consistent, as qualitative data may be subjective and difficult to measure and compare.

Alignment with industry benchmarks is a useful but not critical factor when developing KRIs, as it provides a reference or a standard for comparing the organization's risk level and performance with its peers or competitors. However, alignment with industry benchmarks does not ensure that the KRIs are suitable and feasible for the organization's specific context and capabilities.
References =
Threshold - CIO Wiki
Risk Thresholds: How to Set Them and When to Use Them - ProjectManager.com Risk Appetite and Tolerance - CIO Wiki Risk Reporting - CIO Wiki Regulatory Compliance - CIO Wiki
[Regulatory Risk - CIO Wiki]
[Qualitative Data - CIO Wiki

NEW QUESTION: 778
The PRIMARY purpose of vulnerability assessments is to:
A. provide clear evidence that the system is sufficiently secure.
B. determine the impact of potential threats.
C. test intrusion detection systems (IDS) and response procedures.
D. detect weaknesses that could lead to system compromise.
Answer: (SHOW ANSWER)
The primary purpose of vulnerability assessments is to detect weaknesses that could lead to system compromise. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. By identifying and prioritizing the vulnerabilities, a vulnerability assessment helps to prevent or reduce the risk of cyberattacks that could exploit the vulnerabilities and compromise the system. The other options are not the primary purpose, but they may be secondary or tertiary outcomes or benefits of a vulnerability assessment. Providing clear evidence that the system is sufficiently secure is a result of a successful vulnerability assessment and remediation process, but it is not the main objective. Determining the impact of potential threats is a part of the risk assessment process, which complements the vulnerability assessment process, but it is not the same as detecting the vulnerabilities. Testing intrusion detection systems (IDS) and response procedures is a part of the penetration testing process, which simulates a real-world attack on the system to evaluate its security posture, but it is not the same as scanning the system for vulnerabilities. References = What is Vulnerability Assessment | VA Tools and Best Practices - Imperva

NEW QUESTION: 779
A risk practitioner is performing a risk assessment of recent external advancements in quantum computing. Which of the following would pose the GREATEST concern for the risk practitioner?
A. The organization has not adopted Infrastructure as a Service (IaaS) for its operations
B. The organization has incorporated blockchain technology in its operations
C. The organization has implemented heuristics on its network firewall
D. The organization has not reviewed its encryption standards
Answer: (SHOW ANSWER)

Quantum computing threatens outdated algorithms and key lengths. The biggest concern is stale encryption standards-they directly relate to cryptographic resilience. ISACA materials underscore that encryption evaluation is foundational in emerging-threat risk assessments.

NEW QUESTION: 780

Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

FreeCram.net

A. Service level agreements (SLAs) have not been met over the last quarter.
B. The service contract is up for renewal in less than thirty days.
C. Key third-party personnel have recently been replaced.
D. Monthly service charges are significantly higher than industry norms.
Answer: (SHOW ANSWER)
The observation from a third-party service provider review that would be of greatest concern to a risk practitioner is that the service level agreements (SLAs) have not been met over the last quarter, as it indicates a significant performance issue or breach that may affect the quality, functionality, or security of the outsourced services, and may require a remediation or escalation action. The other options are not the greatest concerns, as they may not indicate a performance issue or breach, but rather a contractual, personnel, or financial issue, respectively, that may not affect the outsourced services directly or significantly.
References = CRISC Review Manual, 7th Edition, page 111.

NEW QUESTION: 781
The BEST way to validate that a risk treatment plan has been implemented effectively is by reviewing:
A. results of a business impact analysis (BIA).
B. the original risk response plan.
C. training program and user awareness documentation.
D. a post-implementation risk and control self-assessment (RCSA).
Answer: (SHOW ANSWER)
A post-implementation RCSA is a process of verifying whether the risk treatment plan has been executed as intended and whether the residual risk is within the acceptable level. It involves testing the effectiveness of the controls that have been implemented to mitigate the risk and identifying any gaps or issues that need to be addressed. A BIA, the original risk response plan, and the training program and user awareness documentation are not sufficient to validate the effectiveness of the risk treatment plan, as they do not measure the actual performance of the controls or the residual risk.
References:
*ISACA, Risk IT Framework, 2nd Edition, 2019, p. 761
*ISACA, Risk and Information Systems Control Review Manual, 7th Edition, 2020, p. 2112

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated**

and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 782
Which of the following will BEST ensure that controls adequately support business goals and objectives?
A. Using the risk management process
B. Enforcing strict disciplinary procedures in case of noncompliance
C. Reviewing results of the annual company external audit
D. Adopting internationally accepted controls
Answer: (SHOW ANSWER)
Using the risk management process will best ensure that controls adequately support business goals and objectives, as it involves identifying, assessing, responding, and monitoring the risks that may affect the achievement of the business goals and objectives, and designing and implementing controls to mitigate those risks. Enforcing strict disciplinary procedures in case of noncompliance, reviewing results of the annual company external audit, and adopting internationally accepted controls are also good practices, but they are not the best, as they do not necessarily align the controls with the business goals and objectives. References = CRISC Review Manual, 7th Edition, page 146.

NEW QUESTION: 783
Which of the following is the BEST source for identifying key control indicators (KCIs)?
A. Privileged user activity monitoring controls
B. Controls mapped to organizational risk scenarios
C. Recent audit findings of control weaknesses
D. A list of critical security processes
Answer: (SHOW ANSWER)
Key control indicators (KCIs) are metrics that provide information on the extent to which a given control is meeting its intended objectives in terms of loss prevention, reduction, etc. In order to provide such information, the control effectiveness indicator has to have an explicit relationship to both the specific control and to the specific risk against which the control has been implemented1. Therefore, the best source for identifying KCIs is to use controls mapped to organizational risk scenarios, which can help define the control objectives, the expected outcomes, and the relevant indicators for each risk scenario. This approach can also help align the KCIs with the organizational goals and strategy, and enable the monitoring and reporting of the control effectiveness23.
The other options are not the best sources for identifying KCIs, because:
Privileged user activity monitoring controls are specific types of controls that aim to prevent unauthorized access or misuse of sensitive data or systems by privileged users. They are not a sourcefor identifying KCIs, but rather a possible subject of KCIs. For example, a KCI for this type of control could be the number of privileged user accounts that have not been reviewed or revoked within a specified period4.
Recent audit findings of control weaknesses are useful for identifying the gaps or deficiencies in the existing control environment, and for recommending corrective actions or improvements. However, they are not a

source for identifying KCIs, but rather an input for evaluating or revising the existing KCIs. For example, if an audit finding reveals that a control is not operating as intended, or that a KCI is not providing reliable or timely information, then the control or the KCI may need to be modified or replaced5.
A list of critical security processes is a high-level overview of the key activities or functions that are essential for maintaining the security of the organization's assets and information. It is not a source for identifying KCIs, but rather a starting point for defining the control objectives and requirements. For example, a critical security process could be incident response, which requires a set of controls to ensure the timely and effective detection, containment, analysis, and recovery of security incidents. The KCIs for this process could be the number of incidents detected, the average time to resolve incidents, or the percentage of incidents that resulted in data breaches6.
References =
Key Control Indicator (KCI) - CIO Wiki
How to Develop Key Control Indicators to Improve Security Risk Monitoring - Gartner Indicators - Program Evaluation - CDC Privileged User Monitoring: What Is It and Why Is It Important? - LogRhythm Internal Audit Key Performance Indicators (KPIs) - AuditBoard Hierarchy of Controls - NIOSH - CDC

NEW QUESTION: 784
Which of the following is the BEST way to determine software license compliance?
A. List non-compliant systems in the risk register.
B. Conduct periodic compliance reviews.
C. Review whistleblower reports of noncompliance.
D. Monitor user software download activity.
Answer: (SHOW ANSWER)
According to the 6 Best Practices to Ensure Software License Compliance article, the best way to determine software license compliance is to conduct regular internal compliance audits. These self-assessments can be done with the help of software license management companies. The goal is to see where compliance issues lie and to take corrective actions before they become serious problems. Periodic compliance reviews can help to avoid fines, penalties, lawsuits, and reputational damage that may result from software license violations.
They can also help to optimize software spending and utilization, and to identify any gaps or opportunities for improvement in the software license management process. References = 6 Best Practices to Ensure Software License Compliance

NEW QUESTION: 785
Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?
A. Survey device owners.
B. Rescan the user environment.
C. Require annual end user policy acceptance.
D. Review awareness training assessment results
Answer: (SHOW ANSWER)

The best way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan is to rescan the user environment, as it provides an objective and reliable way to measure and verify the effectiveness and adequacy of the controls, and to detect any remaining or new vulnerabilities. Surveying device owners, requiring annual end user policy acceptance, and reviewing awareness training assessment results are not the best ways, as they may not provide sufficient assurance, evidence, or timeliness of the control validation, respectively. References = CRISC Review Manual, 7th Edition, page 154.

NEW QUESTION: 786
Which of the following will help ensure the elective decision-making of an IT risk management committee?
A. Key stakeholders are enrolled as members
B. Approved minutes ate forwarded to senior management
C. Committee meets at least quarterly
D. Functional overlap across the business is minimized
Answer: (SHOW ANSWER)
The best way to ensure the effective decision-making of an IT risk management committee is to enroll key stakeholders as members. Key stakeholders are the individuals or groups who have an interest or influence in the IT risk management process, such as business owners, senior management, IT managers, auditors, regulators, customers, and suppliers. By involving key stakeholders in the IT risk management committee, the committee can benefit from their diverse perspectives, expertise, and experience, and ensure that the IT risk management decisions are aligned with the business objectives, priorities, and expectations. Key stakeholders can also provide valuable input, feedback, and support for the IT risk management activities, and help communicate and implement the IT risk management decisions across the organization. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 36.

NEW QUESTION: 787
Following a business continuity planning exercise, an organization decides to accept an identified risk associated with a critical business system. Which of the following should be done next?
A. Document the decision-making process and considerations used
B. Perform a business impact analysis (BIA) to assess the impact of the risk
C. Develop a disaster recovery plan (DRP) and business continuity plan (BCP) to ensure resiliency
D. Develop a control to reduce the level of the risk
Answer: (SHOW ANSWER)
When a risk is accepted, it must be documented in the risk register-including rationale, alternatives evaluated, decision-makers, and contextual factors. This aligns with governance and audit accountability requirements in ISACA guidance.

NEW QUESTION: 788
Which of the following would qualify as a key performance indicator (KPI)?
A. Aggregate risk of the organization
B. Number of identified system vulnerabilities

C. Number of exception requests processed in the past 90 days
D. Number of attacks against the organization's website
Answer: (SHOW ANSWER)
A key performance indicator (KPI) is a measurable value that demonstrates how effectively an organization is achieving its key objectives. A KPI should be relevant, specific, measurable, achievable, and time-bound.
The number of identified system vulnerabilities is a KPI that measures the security posture and performance of the organization's information systems. It also helps to identify the areas that need improvement or remediation.
The number of identified system vulnerabilities is relevant to the organization's objective of protecting its information assets, specific to the system level, measurable by using tools or methods, achievable by implementing security controls or practices, and time-bound by setting a target or threshold. Aggregate risk of the organization, number of exception requests processed in the past 90 days, and number of attacks against the organization's website are not KPIs, as they are either too broad, not relevant, or not measurable.
References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.1.1.1, page 1741
1: ISACA Certified in Risk and Information Systems Control (CRISC) Exam Guide, Answer to Question 647.

NEW QUESTION: 789
Senior management has requested more information regarding the risk associated with introducing a new application into the environment. Which of the following should be done FIRST?
A. Perform an audit.
B. Conduct a risk analysis.
C. Develop risk scenarios.
D. Perform a cost-benefit analysis.
Answer: (SHOW ANSWER)
Understanding Risk Analysis:
* Risk analysis involves identifying potential risks associated with a new application and assessing their likelihood and impact on the organization.
* It provides a detailed understanding of the potential threats, vulnerabilities, and consequences, enabling informed decision-making.
Steps in Conducting a Risk Analysis:
* Identify Risks: Determine what risks could arise from the new application, including security vulnerabilities, compliance issues, and operational disruptions.
* Assess Risks: Evaluate the likelihood and impact of each identified risk. This includes both qualitative and quantitative assessments.
* Prioritize Risks: Rank the risks based on their assessed impact and likelihood to focus on the most significant threats first.
Importance of Risk Analysis:
* Provides senior management with a comprehensive view of the risks involved, enabling them to make informed decisions about proceeding with the application.

* Helps in developing mitigation strategies to address the identified risks.
Comparing Other Options:
* Perform an Audit: Audits are useful for evaluating existing controls but are not the first step in assessing risks for a new application.
* Develop Risk Scenarios: This is part of the risk analysis process but comes after identifying and assessing risks.
* Perform a Cost-Benefit Analysis: Important for decision-making but follows the initial risk analysis to understand potential impacts.
References:
* The CRISC Review Manual emphasizes the importance of conducting a risk analysis to understand and manage risks associated with new applications (CRISC Review Manual, Chapter 2: IT Risk Assessment, Section 2.2.1 Conducting Risk Analysis).

NEW QUESTION: 790

An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

Freecram.net

A. Implement database activity and capacity monitoring.
B. Ensure the business is aware of the risk.
C. Ensure the enterprise has a process to detect such situations.
D. Consider providing additional system resources to this job.
Answer: (SHOW ANSWER)
The risk practitioner's best recommendation is to consider providing additional system resources to this job, as this would help to reduce the likelihood and impact of the risk of delaying financial reporting. Providing additional system resources, such as memory, CPU, disk space, or bandwidth, can improve the performance and efficiency of the application and the scheduled job. This can also help to avoid potential errors, failures, or interruptions that could affect the quality and timeliness of the financial data and reporting.
The other options are not the best recommendations for this situation. Implementing database activity and capacity monitoring is a good practice to identify and analyze the root causes of performance issues, but it does not directly address the risk of delaying financial reporting. Ensuring the business is aware of the risk is an important step to communicate and escalate the risk, but it does not provide a solution or mitigation strategy. Ensuring the enterprise has a process to detect such situations is a preventive measure to avoid or minimize the occurrence of the risk, but it does not eliminate or reduce the risk. References = Practical Recommendations for Better Enterprise Risk Management - ISACA, HR Risk Management: A Practitioner's Guide - AIHR, Isaca CRISC today updated questions - Verified by Isaca Experts

NEW QUESTION: 791
Which of the following is the BEST way to validate the results of a vulnerability assessment?
A. Perform a penetration test.
B. Review security logs.
C. Conduct a threat analysis.

D. Perform a root cause analysis.

Answer: A (LEAVE A REPLY)

According to the CRISC Review Manual (Digital Version), the best way to validate the results of a vulnerability assessment is to perform a penetration test, which is a type of security testing that simulates an attack on the IT assets and processes to exploit the identified vulnerabilities and evaluate the potential impact and severity of the attack. Performing a penetration test helps to:

Confirm the existence and exploitability of the vulnerabilities detected by the vulnerability assessment Measure the effectiveness and efficiency of the existing security controls and countermeasures Identify and prioritize the risks and gaps in the security posture of the IT assets and processes Recommend and implement appropriate remediation and mitigation actions to address the vulnerabilities and risks Enhance the security awareness and resilience of the organization References = CRISC Review Manual (Digital Version), Chapter 1: IT Risk Identification, Section 1.5: IT Risk Identification Methods and Techniques, pp. 36-371

NEW QUESTION: 792

Who is accountable for risk treatment?

A. Enterprise risk management team

B. Risk mitigation manager

C. Business process owner

D. Risk owner

Answer: (SHOW ANSWER)

Risk treatment is the process of selecting and implementing the appropriate risk response strategy and actions to address the identified risks. Risk treatment can involve different strategies, such as avoiding, reducing, transferring, or accepting the risk. Risk owner is the person or group who has the authority and accountability to manage the risk and its response. Risk owner is accountable for risk treatment, as they are responsible for deciding, approving, and executing the risk treatment plan, and for monitoring and reportingthe results and outcomes of the risk treatment. The other options are not accountable for risk treatment, as they have different roles or responsibilities in the risk management process:

Enterprise risk management team is the group of risk managers and practitioners who support the enterprise- wide risk management program, and provide guidance and direction to the risk owners and stakeholders.

Enterprise risk management team may advise or assist the risk owner in risk treatment, but they are not accountable for risk treatment.

Risk mitigation manager is the person who designs, implements, and monitors the risk mitigation actions or measures that reduce the likelihood or impact of the risk to an acceptable level, such as controls, policies, or procedures. Risk mitigation manager may advise or assist the risk owner in risk treatment, but they are not accountable for risk treatment.

Business process owner is the stakeholder who is responsible for the business process that is supported by the IT system or application, such as the CRM system. Business process owner may be affected by or contribute to the risk, and may be involved in the risk treatment, but they are not accountable for risk

treatment, unless they are also the risk owner. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 3, Section 3.1.1.1, pp. 95-96.

NEW QUESTION: 793
Which of the following analyses is MOST useful for prioritizing risk scenarios associated with loss of IT assets?
A. SWOT analysis
B. Business impact analysis (BIA)
C. Cost-benefit analysis
D. Root cause analysis
Answer: (SHOW ANSWER)
Business impact analysis (BIA) is the most useful analysis for prioritizing risk scenarios associated with loss of IT assets, because it evaluates the potential consequences of disruption to critical business functions and processes. BIA helps to identify the most significant risks and the most urgent recovery needs. SWOT analysis, cost-benefit analysis, and root cause analysis are all useful tools for different purposes, but they do not directly address the impact of risk scenarios on business continuity and resilience. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 143

NEW QUESTION: 794
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?
A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects
Answer: (SHOW ANSWER)
A consolidated view into the organization's risk profile is a comprehensive and integrated representation of the risks that may affect the organization's objectives, performance, and value creation12.
The most helpful material to provide a consolidated view into the organization's risk profile is the IT risk register, which is a document that records and tracks the IT-related risks, their sources, impacts, likelihoods, responses, owners, and statuses within the organization34.
The IT risk register is the most helpful material because it provides a complete and consistent overview of the IT risk landscape, and enables the identification, analysis, evaluation, treatment, monitoring, and communication of IT risks across the organization34.
The IT risk register is also the most helpful material because it supports the project prioritization and resource allocation decisions, by highlighting the most significant and relevant IT risks, and by showing the alignment of the IT risk responses with the organization's risk appetite, strategy, and objectives34.
The other options are not the most helpful materials, but rather possible inputs or outputs of the IT risk register. For example:
A list of key risk indicators (KRIs) is a set of metrics that measure the occurrence or status of IT risks, and provide timely and relevant information and feedback to the organization56. However, a list of KRIs is not the

most helpful material because it does not provide a comprehensive and integrated view of the IT risk profile, but rather a snapshot or a trend of selected IT risks56.
Internal audit reports are documents that present the findings and recommendations of the internal audit function, which evaluates the adequacy and effectiveness of the IT risk management and control processes within the organization78. However, internal audit reports are not the most helpful material because they do not provide a comprehensive and integrated view of the IT risk profile, but rather a periodic and independent assessment of specific IT risk areas78.
A list of approved projects is a document that records and tracks the IT projects that have been authorized and funded by the organization, and their objectives, scope, schedule, budget, and status . However, a list of approved projects is not the most helpful material because it does not provide a comprehensive and integrated view of the IT risk profile, but rather a summary of the IT project portfolio . References =
1: Risk IT Framework, ISACA, 2009
2: IT Risk Management Framework, University of Toronto, 2017
3: IT Risk Register Template, ISACA, 2019
4: IT Risk Register Toolkit, ISACA, 2019
5: KPIs for Security Operations & Incident Response, SecurityScorecard Blog, June 7, 2021
6: Key Performance Indicators (KPIs) for Security Operations and Incident Response, DFLabs White Paper, 2018
7: IT Audit and Assurance Standards, ISACA, 2014
8: IT Audit and Assurance Guidelines, ISACA, 2014
IT Project Management Framework, University of Toronto, 2017
IT Project Management Best Practices, ISACA Journal, Volume 1, 2018

NEW QUESTION: 795
Which of the following approaches MOST effectively enables accountability for data protection?
A. Establishing ownership for data within applications and systems
B. Establishing discipline for policy violations by data owners
C. Implementing data protection policies across the organization
D. Conducting data protection awareness and training campaigns
Answer: (SHOW ANSWER)
Assigning ownership ensures accountability, as data owners are responsible for ensuring appropriate protections are in place and enforced.
Reference:CRISC Manual - Domain 1, Slide 403, 471

NEW QUESTION: 796
Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?
A. To support regulatory requirements
B. To prevent the risk scenario in the current environment
C. To monitor for potential changes to the risk scenario
D. To track historical risk assessment results

Answer: (SHOW ANSWER)

A risk register is a document that records and tracks the identified risks, their causes, impacts, likelihood, responses, and status. A risk register can help manage and communicate risks throughout the risk management process. A risk register should be updated regularly to reflect the current state of risks and their responses. Due to a change in business processes, an identified risk scenario may no longer require mitigation, as the risk level may have decreased or the risk may have been eliminated. However, the risk should remain in the risk register, as the most important reason is to monitor for potential changes to the risk scenario. This means keeping track of the internal and external factors that may affect the risk scenario, such as new threats, vulnerabilities, opportunities, or controls. Monitoring for potential changes to the risk scenario can help identify and respond to any emerging or reoccurring risks, and ensure that therisk register is accurate and complete. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, Section 1.3: Risk Register, p. 41-43.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 797

An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:

A. senior management has oversight of the process.

B. process ownership aligns with IT system ownership.

C. segregation of duties exists between risk and process owners.

D. risk owners have decision-making authority.

Answer: (SHOW ANSWER)

According to the 1.9 Ownership & Accountability - CRISC, risk ownership is best established by mapping risk to specific business process owners. Details of the risk owner should be documented in the risk register. Results of the risk monitoring should be discussed and communicated with the risk owner as they own the risk and are accountable for maintaining the risk within acceptable levels. To ensure effective risk ownership, it is most important that risk owners have decision-making authority, as this enables them to take timely and appropriate actions to manage the risk and ensure that it is aligned with the organization's risk appetite and tolerance. Without decision-making authority, risk owners may not be able to implement the necessary risk responses or escalate the issues to the relevant stakeholders. Therefore, the answer is D. risk owners have decision-making authority. References = 1.9 Ownership & Accountability - CRISC, The Importance of Effective Risk Governance in the C-suite - Aon

NEW QUESTION: 798

Which of the following BEST enables the timely detection of changes in the security control environment?
A. Control self-assessment (CSA)
B. Log analysis
C. Security control reviews
D. Random sampling checks
Answer: (SHOW ANSWER)
Understanding the Question:
The question asks which method best enables timely detection of changes in the security control environment.
Analyzing the Options:
A). Control self-assessment (CSA):Allows for continuous monitoring and quick detection of any changes or deficiencies in controls.
B). Log analysis:Useful for detecting security incidents but not as comprehensive as CSA for overall control environment changes.
C). Security control reviews:Typically periodic and might not be as timely.
D). Random sampling checks:Not as systematic or comprehensive as CSA.
Control Self-Assessment (CSA):CSA involves regular, structured evaluations by internal staff to ensure controls are working effectively. It promotes early detection of issues by those directly responsible for the controls.
Timeliness:CSA is an ongoing process, making it more timely in identifying changes compared to periodic reviews or random checks.
References:
CRISC Review Manual, Chapter 3: Risk Response and Reporting, emphasizes the importance of CSA in maintaining and improving control environments.

NEW QUESTION: 799
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:
A. is in charge of information security.
B. is responsible for enterprise risk management (ERM)
C. can implement remediation action plans.
D. is accountable for loss if the risk materializes.
Answer: (SHOW ANSWER)
According to the CRISC Review Manual, a risk owner is the person who is accountable for the risk and its associated mitigation actions. The risk owner is responsible for monitoring the risk, reporting the risk status, and implementing the risk response. Therefore, the most appropriate risk owner would be the individual who is accountable for loss if the risk materializes, as it implies that they have the authority and the incentive to manage the risk effectively. The other options are not the most appropriate risk owners, as they are not directly accountable for the risk or its consequences. The person who is in charge of information security is responsible for overseeing the IT security function and ensuring that the IT security policy is enforced, but they may not have the authority or the resources to manage the risk. The person who is responsible for

enterprise risk management (ERM) is responsible for establishing and maintaining the ERM framework and processes, but they may not have the knowledge or the involvement to manage the risk. The person who can implement remediation action plans is responsible for executing the risk response, but they may not have the decision-making power or the accountability to manage the risk. References = CRISC Review Manual, 7th Edition, Chapter 3, Section 3.1.2, page 108.

NEW QUESTION: 800

An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

Pgcram.net

A. Data retention requirements
B. Data destruction requirements
C. Cloud storage architecture
D. Key management
Answer: (SHOW ANSWER)
The most important factor to consider when assessing the residual risk of implementing encryption for data at rest is the key management. Key management is the process of generating, storing, distributing, using, and destroying the cryptographic keys that are used to encrypt and decrypt the data. Key management is essential for ensuring the security, availability, and integrity of the encrypted data, as well as for complying with the legal and regulatory requirements. Poor key management could result in the loss, theft, compromise, or corruption of the keys, which could lead to unauthorized access, data breach, data loss, or data recovery failure. Therefore, key management must be considered to assess the residual risk, which is the risk that remains after the risk treatment, such as encryption, is applied. Data retention requirements, data destruction requirements, and cloud storage architecture are not as important as key management, as they do not directly affect the encryption and decryption of the data, and they may not introduce significant residual risk. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 217.

NEW QUESTION: 801
Which of the following is the MOST important reason for an organization to regularly assess the design of key risk indicators (KRIs)?
A. Increasing process failures could impact a key objective.
B. Tolerance levels change as strategies evolve.
C. System enhancements could bypass the change control process.
D. Data required for risk reporting changes with industry trends.
Answer: (SHOW ANSWER)
As strategies evolve, so do the acceptable risk thresholds (tolerances). Regular KRI reassessment ensures alignment with the current risk appetite and supports timely, risk-informed decisions.
Reference:CRISC Manual - Domain 4, Slide 384-386

NEW QUESTION: 802
Which of the following will BEST support management repotting on risk?
A. Risk policy requirements

B. A risk register
C. Control self-assessment
D. Key performance Indicators
Answer: (SHOW ANSWER)
Key performance indicators (KPIs) are metrics that measure the achievement of objectives and the effectiveness of processes. KPIs can help management report on risk by providing quantitative and qualitative information on the risk profile, the risk appetite, the risk response, and the risk outcomes. KPIs can also help monitor and communicate the progress and results of risk management activities, such as risk identification, assessment, mitigation, and reporting. KPIs can be aligned with the strategic, operational, and tactical goals of the organization, and can be tailored to the specific needs and expectations of different stakeholders. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section 4.2: Key Risk Indicators and Key Performance Indicators, p. 197-199.

NEW QUESTION: 803
Which of the following is the MOST important input when developing risk scenarios?
A. Key performance indicators
B. Business objectives
C. The organization's risk framework
D. Risk appetite
Answer: (SHOW ANSWER)
The most important input when developing risk scenarios is the business objectives, as they provide the context and scope for the risk identification and analysis process. Risk scenarios are hypothetical situations that describe the possible causes, events, and consequences of a risk. Risk scenarios help to understand and communicate the nature and impact of the risk, and to support the risk assessment and response planning. The business objectives are the goals and targets that the organization wants to achieve through its processes, functions, and projects. The business objectives define the expected outcomes and performance of the organization, and the criteria for measuring and evaluating the success or failure of the organization. The business objectives also reflect the organization's vision, mission, values, and strategy, and the needs and expectations of the stakeholders. The other options are not the most important inputs when developing risk scenarios, although they may be useful or relevant information. Key performance indicators are metrics that measure and monitor the progress and achievement of the business objectives, but they do not provide the context or scope for the risk scenarios. The organization's risk framework is the set of principles, policies, and processes that guide and support the risk management activities across the organization, but it does not provide the context or scope for the risk scenarios. Risk appetite is the level of risk that the organization is willing to accept or avoid in pursuit of its business objectives, but it does not provide the context or scope for the risk scenarios. References = Risk and Information Systems Control Study Manual, Chapter 2: IT Risk Identification, page 58.

NEW QUESTION: 804

A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

A. Single sign-on

B. Audit trail review

C. Multi-factor authentication

D. Data encryption at rest

Answer: C (LEAVE A REPLY)

Multi-factor authentication is the most effective way to mitigate the risk of unauthorized access to the system, as it requires the users to provide more than one piece of evidence to prove their identity, such as a password, a token, a biometric feature, etc. This reduces the likelihood of compromising the credentials and ensures that only authorized users can perform maintenance on the system.

Single sign-on is a convenience feature that allows users to access multiple systems with one set of credentials, but it does not address the risk of sharing credentials among multiple users.

Audit trail review is a detective control that can help identify and investigate unauthorized access to the system, but it does not prevent or mitigate the risk of credential compromise.

Data encryption at rest is a security measure that protects the data stored on the system from unauthorized access, but it does not prevent or mitigate the risk of credential compromise. References = CRISC Review Manual, 7th Edition, ISACA, 2020, page 107-108.

NEW QUESTION: 805

Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

A. Occurrences of specific events

B. A performance measurement

C. The risk tolerance level

D. Risk scenarios

Answer: (SHOW ANSWER)

Occurrences of specific events are the most likely to cause a key risk indicator (KRI) to exceed thresholds, as they represent the actual or potential realization of the risk. A KRI is a metric that measures the level of risk exposure and the effectiveness of risk response strategies, and it has predefined thresholds that indicate the acceptable or unacceptable risk status. When a specific event occurs that affects the risk, such as a security breach, a system failure, or a compliance violation, the KRI value may change and exceed the thresholds, triggering an alert or an action. A performance measurement, the risk tolerance level, and risk scenarios are not the most likely to cause a KRI to exceed thresholds, as they do not reflect the actual or potential occurrence of the risk, but rather the expected or desired outcome, limit, or simulation of the risk. References = [CRISC Review Manual (Digital Version)], page 121; CRISC by Isaca Actual Free Exam Q&As, question 217.

NEW QUESTION: 806

Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

A. An updated risk register
B. Risk assessment results
C. Technical control validation
D. Control testing results
Answer: (SHOW ANSWER)
Control testing is the process of verifying that the risk mitigation controls are designed and operating effectively, and that they achieve the intended objectives and outcomes. Control testing can involve various methods, such as observation, inspection, inquiry, re-performance, or simulation. Control testing results can provide evidence and assurance that the implementation of a risk mitigation control has been completed as intended, and that the control is functioning properly and consistently. Control testing results can also identify any issues or deficiencies in the control design or operation, and recommend corrective actions or improvements. The other options are not as helpful as control testing results, because they do not provide a direct and objective verification of the control implementation, but rather focus on other aspects or outputs of the risk management process, as explained below:
A). An updated risk register is a document that records and tracks the identified risks, their characteristics, and their status. An updated risk register can reflect the changes in the risk profile and exposure after the implementation of a risk mitigation control, but it does not verify that the control implementation has been completed as intended, or that the control is effective and reliable.
B). Risk assessment results are the outputs of the risk analysis and evaluation process, which measure the impact and likelihood of the risks, and assign a risk rating and priority. Risk assessment results can indicate the level of risk exposure and the need for risk mitigation controls, but they do not verify that the control implementation has been completed as intended, or that the control is effective and reliable.
C). Technical control validation is the process of ensuring that the technical aspects of a control, such as hardware, software, or network components, are configured and functioning correctly. Technical control validation can verify that the control implementation meets the technical specifications and requirements, but it does not verify that the control implementation has been completed as intended, or that the control is effective and reliable from a businessperspective. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.3, page 130.

NEW QUESTION: 807
When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:
A. cost-benefit analysis.
B. risk appetite.
C. regulatory guidelines
D. control efficiency
Answer: (SHOW ANSWER)
Cost-benefit analysis is the most helpful tool to show risk reduction based on when developing risk treatment alternatives for a business case, because it compares the expected costs and benefits of each alternative and helps to select the most optimal and feasible one. Cost-benefit analysis also helps to justify the

investment and resources required for the risk treatment plan and to demonstrate the value and return of the risk reduction.
The other options are not the most helpful tools, although they may also be considered when developing risk treatment alternatives. Risk appetite, regulatory guidelines, and control efficiency are examples of factors or criteria that influence the selection of risk treatment alternatives, but they do not show the risk reduction based on the alternatives. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 808
Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?
A. Regulatory compliance
B. Risk ownership
C. Best practices
D. Desired risk level
Answer: (SHOW ANSWER)
The most important factor to communicate to senior management during the initial implementation of a risk management program is the desired risk level, which is the level of risk that the organization aims to achieve in order to fulfill its objectives and strategy1. The desired risk level can help to:
* Define and communicate the risk appetite and tolerance, which are the amount and type of risk that the organization is willing to accept or pursue in order to achieve its objectives2.
* Guide and align the risk identification, analysis, evaluation, and treatment processes, and ensure that the risks are consistent and proportional to the desired risk level3.
* Measure and monitor the risk performance and outcome, and ensure that the actual risk level is within the desired risk level, or take corrective actions if needed4.
The other factors are not the most important to communicate to senior management, because:
* Regulatory compliance is a necessary but not sufficient factor to communicate to senior management, as it ensures that the risk management program complies with the applicable laws, rules, or standards that govern the organization's activities and operations5. However, regulatory compliance does not guarantee that the risk management program is relevant and useful for the organization's specific objectives and strategy.
* Risk ownership is a desirable but not essential factor to communicate to senior management, as it assigns the roles and responsibilities for managing the risks and implementing the risk responses to the appropriate individuals or entities within the organization. However, risk ownership does not ensure that the risk management program is effective and efficient in achieving the desired risk level.
* Best practices are a useful but not critical factor to communicate to senior management, as they provide the guidelines and standards for designing and implementing the risk management program, based on the experience and knowledge of the industry or the profession. However, best practices do not ensure that the risk management program is suitable and feasible for the organization's specific context and capabilities.
References =
* Desired Risk Level - CIO Wiki
* Risk Appetite and Tolerance - CIO Wiki

* Risk Management Process - CIO Wiki
* Risk Monitoring - CIO Wiki
* Regulatory Compliance - CIO Wiki
* [Risk Ownership - CIO Wiki]
* [Best Practice - CIO Wiki]
* [Risk Management - CIO Wiki]

NEW QUESTION: 809
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?
A. Implement user access controls
B. Perform regular internal audits
C. Develop and communicate fraud prevention policies
D. Conduct fraud prevention awareness training.
Answer: C (LEAVE A REPLY)
Developing and communicating fraud prevention policies is the most effective way to reduce potential losses due to ongoing expense fraud because it creates a culture of integrity and accountability, sets clear expectations and consequences for employees, and deters fraudulent behavior. Implementing user access controls, performing regular internal audits, and conducting fraud prevention awareness training are also important controls, but they are more reactive and detective than preventive. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 4-26.

NEW QUESTION: 810
The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:
FreeCram.net
A. detected incidents.
B. residual risk.
C. vulnerabilities.
D. inherent risk.
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after applying risk responses, such as avoidance, mitigation, transfer, or acceptance. It represents the level of exposure that the organisation is willing to tolerate or assume. Residual risk should be aligned with the organisation's risk appetite and risk tolerance, which are determined by senior management. Therefore, the best way to obtain senior management support for investment in a control implementation would be to articulate the reduction in residual risk that the control would achieve. This would demonstrate how the control would help the organisation meet its risk objectives and reduce the likelihood or impact of adverse events. References = ISACA CRISC Review Manual, 7th Edition, Chapter 1, Section 1.3.2, page 25.

NEW QUESTION: 811

An organization is measuring the effectiveness of its change management program to reduce the number of unplanned production changes. Which of the following would be the BEST metric to determine if the program is performing as expected?

A. Decrease in the time to move changes to production

B. Ratio of emergency fixes to total changes

C. Ratio of system changes to total changes

D. Decrease in number of changes without a fallback plan

Answer: (SHOW ANSWER)

The ratio of emergency fixes to total changes is the best metric to determine if the change management program is performing as expected, because it reflects the quality and stability of the changes that are implemented in the production environment. A high ratio of emergency fixes to total changes indicates that the change management program is not effective, as it means that many changes are causing problems or failures that require urgent correction. A low ratio of emergency fixes to total changes indicates that the change management program is effective, as it means that most changes are well-planned, tested, and approved, and do not cause significant disruptions or defects. The ratio of emergency fixes to total changes can also help identify the root causes of the problems, the gaps in the change management process, and the areas for improvement. For example, if the ratio of emergency fixes to total changes is high, it may indicate that the change management program has issues with the following aspects: - Change request and approval: The change management program may not have a clear and consistent process for requesting, reviewing, and approving changes, or the process may not be followed by all stakeholders. - Change impact analysis: The change management program may not have a comprehensive and systematic method for assessing the potential impact of the changes on the business processes, the IT systems, the users, and the customers. - Change testing and validation: The change management program may not have adequate testing and validation procedures to ensure that the changes meet the requirements and specifications, and do not introduce errors or vulnerabilities. - Change communication and training: The change management program may not have effective communication and training strategies to inform and educate the affected parties about the changes and their implications. - Change implementation and monitoring: The change management program may not have proper implementation and monitoring plans or tools to ensure that the changes are executed smoothly and successfully, and that any issues or incidents are detected and resolved promptly. Therefore, the ratio of emergency fixes to total changes is the best metric to determine if the change management program is performing as expected, as it can provide valuable feedback and insights for the change management program and its improvement. References = How to Measure Change Management Effectiveness: Metrics, Tools & Processes1, Metrics for Measuring Change Management2, Driving Value with Change Management Metrics3, Must-Know Organizational Change Management Metrics

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here:

https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 812
Which of the following BEST enables the integration of IT risk management across an organization?
A. Enterprise risk management (ERM) framework
B. Enterprise-wide risk awareness training
C. Robust risk reporting practices
D. Risk management policies
Answer: (SHOW ANSWER)
Understanding the Question:
The question asks what best enables the integration of IT risk management across an organization.
Analyzing the Options:
A). Enterprise risk management (ERM) framework:Provides a comprehensive approach to integrating risk management across the entire organization.
B). Enterprise-wide risk awareness training:Important for education but doesn't ensure integration.
C). Robust risk reporting practices:Crucial for communication but not integration.
D). Risk management policies:Necessary but need to be part of an overall framework for effective integration.
ERM Framework:An ERM framework ensures that risk management practices are standardized and integrated throughout the organization. It aligns risk management with business objectives, ensuring that IT risk is considered within the broader context of enterprise risk.
Comprehensive Approach:ERM covers all aspects of risk, including IT, and facilitates a unified approach to managing risk across all departments and levels.
References:
CRISC Review Manual, Chapter 1: Governance, details the role of an ERM framework in integrating risk management practices across an organization.

NEW QUESTION: 813
A business is conducting a proof of concept on a vendor's AI technology. Which of the following is the MOST important consideration for managing risk?
A. Use of a non-production environment
B. Regular security updates
C. Third-party management plan
D. Adequate vendor support
Answer: A (LEAVE A REPLY)
Conducting a proof of concept in a non-production environment ensures that any potential issues or vulnerabilities in the AI technology do not affect live systems or data. This approach allows for thorough testing and evaluation without risking operational disruptions or data breaches.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 4: Information Technology and Security, Section: IT Risk Mitigation Strategies.

NEW QUESTION: 814
Which of the following is the BEST way to determine the value of information assets for risk management purposes?
A. Assess the loss impact if the information is inadvertently disclosed.
B. Calculate the overhead required to keep the information secure throughout its life cycle.
C. Calculate the replacement cost of obtaining the information from alternate sources.
D. Assess the market value offered by consumers of the information.
Answer: (SHOW ANSWER)
The best way to determine the value of information assets for risk management purposes is to assess the loss impact if the information is inadvertently disclosed, as this reflects the potential damage or harm that the organization may suffer due to a breach of confidentiality, integrity, or availability of the information. The loss impact can be measured in terms of financial, operational, reputational, legal, or regulatory consequences, depending on the nature, sensitivity, and criticality of the information. The loss impact can also help the organization to prioritize the protection and mitigation of the information assets, and to align the risk management strategy with the business objectives and risk appetite.
References:
*ISACA, IT Asset Valuation, Risk Assessment and Control Implementation Model1
*ISACA, Data Classification: What It Is, Why You Should Care and How to Perform It2

NEW QUESTION: 815
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?
A. Control self-assessment (CSA)
B. Security information and event management (SIEM) solutions
C. Data privacy impact assessment (DPIA)
D. Data loss prevention (DLP) tools
Answer: (SHOW ANSWER)
Software as a service (SaaS) is a cloud computing model that provides software applications over the internet, without requiring the customer to install or maintain them on their own devices1. SaaS applicationscan offer many benefits, such as scalability, accessibility, and cost-efficiency, but they also pose security risks, such as data breaches, unauthorized access, and compliance violations2.
One of the best ways to protect an organization against breaches when using a SaaS application is to use data loss prevention (DLP) tools. DLP tools are software solutions that monitor, detect,and prevent the unauthorized transmission or leakage of sensitive data from an organization's network or devices3. DLP tools can help an organization to:
Identify and classify sensitive data, such as personal information, intellectual property, or financial records, and apply appropriate policies and controls to protect them Encrypt data in transit and at rest, and use secure protocols and encryption keys to ensure data confidentiality and integrity Block or alert on suspicious or malicious data transfers, such as unauthorized uploads, downloads, or sharing of data to external sources or devices Audit and report on data activities and incidents, and provide evidence for compliance with data

protection regulations and standards, such as GDPR, HIPAA, or PCI-DSS4 References = What is SaaS?, Top 7 SaaS Security Risks (and How to Fix Them), What is Data Loss Prevention (DLP)?, Data Loss Prevention (DLP) for SaaS Applications

NEW QUESTION: 816
An organization has built up its cash reserves and has now become financially able to support additional risk while meeting its objectives. What is this change MOST likely to impact?
A. Risk profile
B. Risk capacity
C. Risk indicators
D. Risk tolerance
Answer: (SHOW ANSWER)
Risk capacity is the amount of risk that an organization can financially afford to take, without jeopardizing its ability to meet its objectives or obligations. Risk capacity is determined by factors such as the organization's income, assets, liabilities, and cash flow. An organization that has built up its cash reserves has increased its risk capacity, as it has more financial resources and flexibility to support additional risk. This may enable the organization to pursue more opportunities or initiatives that involve higher risk and higher reward.
Risk profile is a summary of the key risks that an organization faces, and their implications for the organization's objectives and strategy. Risk profile may change due to factors such as new technologies, business initiatives, or external events, but not necessarily due to changes in cash reserves.
Risk indicators are metrics or indicators that help to monitor and evaluate the likelihood or impact of a risk, or the effectiveness or efficiency of a control. Risk indicators may vary depending on the risk sources, scenarios, or responses, but not necessarily due to changes in cash reserves.
Risk tolerance is the amount of risk that an organization is willing to accept, based on its risk appetite and risk capacity. Risk tolerance is influenced by factors such as the organization's culture, values, and objectives, as well as the risk environment and expectations. Risk tolerance may change due to changes in cash reserves, but it is not the most likely impact, as it also depends on the organization's risk appetite and other factors.

NEW QUESTION: 817
The MOST important consideration when selecting a control to mitigate an identified risk is whether:
A. the cost of control exceeds the mitigation value
B. there are sufficient internal resources to implement the control
C. the mitigation measures create compounding effects
D. the control eliminates the risk
Answer: (SHOW ANSWER)
The most important consideration when selecting a control to mitigate an identified risk is whether the cost of control exceeds the mitigation value, because this determines the cost-benefit ratio of the control. A control should not be implemented if the cost of implementing and maintaining it is higher than the expected benefit of reducing the risk exposure. The other options are not the most important considerations, although they may also influence the control selection process. The availability of internal resources, the potential

compounding effects, and the possibility of eliminating the risk are secondary factors that depend on the cost and value of the control. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 818
To reduce costs, an organization is combining the second and third tines of defense in a new department that reports to a recently appointed C-level executive. Which of the following is the GREATEST concern with this situation?
A. The risk governance approach of the second and third lines of defense may differ.
B. The independence of the internal third line of defense may be compromised.
C. Cost reductions may negatively impact the productivity of other departments.
D. The new structure is not aligned to the organization's internal control framework.
Answer: (SHOW ANSWER)
The greatest concern with the situation of combining the second and third lines of defense in a new department that reports to a recently appointed C-level executive is that the independence of the internal third line of defense may be compromised. The second line of defense is the function that oversees and supports the risk management activities of the first line of defense, which is the function that owns and manages the risks.
The third line of defense is the function that provides independent assurance of the risk management activities, such as the internal audit function. Combining the second and third lines of defense in a new department may compromise the independence of the internal third line of defense, as it may create a conflict of interest, bias, or influence among the functions, and impair the objectivity, credibility, and quality of the assurance activities. The independence of the internal third line of defense is essential for ensuring that the risk management activities are performed in a consistent and effective manner, and that the issues and gaps are identified and reported without fear or favor. The risk governance approach of the second and third lines of defense may differ, cost reductions may negatively impact the productivity of other departments, and the new structure may not be aligned to the organization's internal control framework are also concerns, but they are not as great as the compromise of the independence of the internal third line of defense, as they do not directly affect the assurance and accountability of the risk management activities. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 36.

NEW QUESTION: 819
Prudent business practice requires that risk appetite not exceed:
A. inherent risk.
B. risk tolerance.
C. risk capacity.
D. residual risk.
Answer: (SHOW ANSWER)
Risk appetite is the amount and type of risk that an organization is willing to accept in order to achieve its objectives. Risk appetite reflects the organization's risk attitude and its willingness to take on risk in specific scenarios. Risk appetite is usually expressed in a qualitative statement approved by the board of directors1.

Risk capacity is the maximum amount of risk that an organization can responsibly take on without jeopardizing its financial stability or other key objectives. Risk capacity is determined by objective factors like income, assets, liabilities, debts, insurance coverage, dependents, and time horizon. Risk capacity is usually expressed in a quantitative measure that sets the limit of how much risk the organization can handle2.
Prudent business practice requires that risk appetite not exceed risk capacity, because this would mean that the organization is taking on more risk than it can afford or sustain. If the risk appetite is higher than the risk capacity, the organization may face serious consequences such as insolvency, bankruptcy, reputational damage, legal liability, or regulatory sanctions. Therefore, the organization should align its risk appetite with its risk capacity, and ensure that its risk exposure is within its risk tolerance3.
The other options are not correct. Inherent risk is the level of risk that exists in the absence of controls or mitigations. It is the natural level of risk inherent in a process or activity. Residual risk is the level of riskthat remains after the controls or mitigations have been applied. It is the remaining risk after the risk response has been implemented. Risk tolerance is the acceptable variation in the outcomes related to specific objectives or risks. It is the range of risk exposure that the organization is prepared to accept4. None of these concepts are directly comparable to risk appetite, and none of them represent the limit of how much risk the organization can take on. References = Risk Appetite vs. Risk Tolerance: What is the Difference? - ISACA
What Is the Difference Between Risk Tolerance and Risk Capacity? - Investopedia Risk Management: Understanding Risk Capacity, Appetite, and Tolerance - Consulting Edge
[CRISC Review Manual, 7th Edition]

NEW QUESTION: 820

What is a risk practitioner's BEST approach to monitor and measure how quickly an exposure to a specific risk can affect the organization?

Freecram.net

A. Create an asset valuation report.
B. Create key performance indicators (KPIs).
C. Create key risk indicators (KRIs).
D. Create a risk volatility report.
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics that measure the exposure to a given risk at a particular time. They can also provide early warning signs of a potential change in risk level. By monitoring KRIs, risk practitioners can assess how quickly an exposure to a specific risk can affect the organization and take appropriate actions.
References
*Risk management at the speed of business - PwC
*Risk velocity measures how fast an exposure can affect an organization | Business Insurance

NEW QUESTION: 821
Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?
A. KPIs measure manual controls, while KCIs measure automated controls.
B. KPIs and KCIs both contribute to understanding of control effectiveness.
C. A robust KCI program will replace the need to measure KPIs.

D. KCIs are applied at the operational level while KPIs are at the strategic level.

Answer: B (LEAVE A REPLY)

Key performance indicators (KPIs) are metrics or measures that provide information on the progress and performance of an organization or a team toward an intended result or objective. KPIs can help to monitor and evaluate the achievement of strategic, operational, or tactical goals, and to support the decision making and improvement of the organization or the team1.

Key control indicators (KCIs) are metrics or measures that provide information on the status and effectiveness of the controls or safeguards that are implemented to manage the risks or threats that an organization or a team faces. KCIs can help to identify and assess the strengths and weaknesses of the controls or safeguards, and to ensure the compliance and accountability of the organization or the team2.

The statement that best illustrates the relationship between KPIs and KCIs is that KPIs and KCIs both contribute to understanding of control effectiveness, because they can help to:

Measure and compare the actual and expected outcomes and impacts of the controls or safeguards, and to determine the gaps or deviations Analyze and understand the causes and consequences of the gaps or deviations, and to identify the root problems or issues Evaluate and report the performance and compliance of the controls or safeguards, and to communicate the results and feedback to the stakeholders Improve and optimize the design and implementation of the controls or safeguards, and to enhance the efficiency and effectiveness of the risk management process34 The other statements do not illustrate the relationship between KPIs and KCIs accurately, but rather some of the differences or misconceptions between them.

KPIs measure manual controls, while KCIs measure automated controls is a difference between KPIs and KCIs, but not a general one. KPIs and KCIs can measure both manual and automated controls, depending on the type and nature of the controls or safeguards.A robust KCI program will replace the need to measure KPIs is a misconception about KPIs and KCIs, as they are not mutually exclusive or substitutable. KPIs and KCIs complement and support each other, as they provide different but related information on the performance and risk management of the organization or the team.

KCIs are applied at the operational level while KPIs are at the strategic level is a difference between KPIs and KCIs, but not a universal one. KPIs and KCIs can be applied at different levels of the organization or the team, depending on the scope and purpose of the measurement and evaluation. References = Key Performance Indicator (KPI): Definition, Types, and Examples Key Control Indicators - ISACA Key Control Indicators: What They Are and How to Use Them Key Performance Indicators vs. Key Control Indicators: What's the Difference?

[CRISC Review Manual, 7th Edition]

NEW QUESTION: 822

A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner recommend be done NEXT?

A. Implement targeted awareness training for new BYOD users.

B. Implement monitoring to detect control deterioration.

C. Identify log sources to monitor BYOD usage and risk impact.

D. Reduce the risk tolerance level.

Answer: (SHOW ANSWER)

A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. This means that the potential benefits of BYOD outweigh the potential risks, and that the controls in place are adequate to mitigate those risks.

The next step for the risk practitioner is to identify log sources to monitor BYOD usage and risk impact. Log sources are records of events or activities that occur in a system or network, such as file access, network traffic, user behavior, etc. Log sources can provide valuable information about how BYOD devices are used, what data they access, what applications they run, what threats they encounter, etc.

By monitoring log sources, the risk practitioner can track and measure the actual performance and security of BYOD devices, compare them with the expected outcomes and standards, identify any deviations or anomalies that may indicate a breach or a vulnerability, and take appropriate actions to address them.

Therefore, identifying log sources to monitor BYOD usage and risk impact is a recommended action after a successful risk assessment.

The references for this answer are:

Risk IT Framework, page 10

Information Technology & Security, page 4

Risk Scenarios Starter Pack, page 2

NEW QUESTION: 823

Which of the following would BEST support the integrity of online financial transactions?

A. Developing an integrated audit facility

B. Implementing audit trail logs

C. Deploying multi-factor authentication (MFA)

D. Implementing blockchain technology

Answer: (SHOW ANSWER)

Multi-factor authentication (MFA)significantly enhances transaction integrity by ensuring that users are who they claim to be. It is a practical, widely adopted control to prevent unauthorized access.

Reference:CRISC Manual - Domain 3, Slide 276-278

NEW QUESTION: 824

Which of the following BEST prevents unauthorized access to customer personal data transmitted to third-party service providers?

A. Ensuring service providers comply with laws and regulations

B. Reviewing and testing service providers' business continuity plans (BCPs)

C. Implementing and reviewing data sharing controls

D. Requiring service providers to report privacy breaches

Answer: (SHOW ANSWER)

NEW QUESTION: 825

Which of the following is the MOST important consideration when prioritizing risk response?

A. Requirements for regulatory obligations.

B. Cost of control implementation.
C. Effectiveness of risk treatment.
D. Number of risk response options.
Answer: (SHOW ANSWER)
The effectiveness of risk treatment determines whether the selected response sufficiently mitigates the identified risk. This consideration ensures alignment with risk appetite and reduces residual risk to acceptable levels, reflecting the priorities set out in theRisk Response and Treatmentdomain of CRISC.

NEW QUESTION: 826
After undertaking a risk assessment of a production system, the MOST appropriate action is fcr the risk manager to
A. recommend a program that minimizes the concerns of that production system.
B. inform the process owner of the concerns and propose measures to reduce them.
C. inform the IT manager of the concerns and propose measures to reduce them.
D. inform the development team of the concerns and together formulate risk reduction measures.
Answer: (SHOW ANSWER)
The most appropriate action for the risk manager to take after undertaking a risk assessment of a production system is to inform the process owner of the concerns and propose measures to reduce them, as the process owner has the authority and responsibility to manage the production system and its associated risks and controls, and to decide on the optimal risk response. Recommending a program that minimizes the concerns of that production system, informing the IT manager of the concerns and proposing measures to reduce them, and informing the development team of the concerns and together formulating risk reduction measures are not the most appropriate actions, as they may not involve the process owner, who is the key stakeholder and decision maker for the production system and its risks. References = CRISC Review Manual, 7th Edition, page 101.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 827
Which of the following is the MOST important consideration when determining the appropriate data retention period throughout the data management life cycle?
A. Data storage and collection methods
B. Data owner preferences
C. Legal and regulatory requirements
D. Choice of encryption algorithms

Answer: (SHOW ANSWER)
Legal and regulatory requirements are paramount when determining data retention periods. Compliance with laws such as GDPR, HIPAA, or industry-specific regulations ensures that data is retained appropriately and disposed of when no longer necessary, thereby mitigating legal risks.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 2: IT Risk Assessment, Section: Data Management and Privacy.

NEW QUESTION: 828
The operational risk associated with attacks on a web application should be owned by the individual in charge of:
A. network operations.
B. the cybersecurity function.
C. application development.
D. the business function.
Answer: (SHOW ANSWER)
The operational risk associated with attacks on a web application should be owned by the individual in charge of the business function, because they are the primary stakeholder and beneficiary of the web application, and they are responsible for defining and achieving the business objectives and requirements that the web application supports or enables. An operational risk is a risk of loss or damage resulting from inadequate or failed internal processes, people, or systems, or from external events. An attack on a web application is a type of operational risk that involves a malicious or unauthorized attempt to compromise the confidentiality, integrity, or availability of the web application, such as a denial-of-service attack, a SQL injection attack, or a cross-site scripting attack. A web application is an application that runs on a web server and can be accessed or used through a web browser, such as an online shopping site, a social media platform, or a web-based email service. A business function is a set of activities or tasks that support or enable the organization's vision, mission, and strategy, such as marketing, sales, or customer service. A risk owner is a person or role that has the authority and accountability to manage a specific risk, and to implement and monitor the risk response and controls. The individual in charge of the business function should be the risk owner, as they have the best understanding and interest of the web application and its business value and impact, and they have the ability and responsibility to manage the operational risk associated with the attacks on the web application. The individual in charge of network operations, the cybersecurity function, or application development are all possible candidates for the risk owner, but they are not the best choice, as they may not have the same level of stake and influence in the web application and its business objectives and requirements, and they may have different or conflicting priorities or perspectives on the operational risk and its management. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.1, page 101

NEW QUESTION: 829
The PRIMARY objective of testing the effectiveness of a new control before implementation is to:
A. ensure that risk is mitigated by the control.
B. measure efficiency of the control process.

C. confirm control alignment with business objectives.

D. comply with the organization's policy.

Answer: (SHOW ANSWER)

The primary objective of testing the effectiveness of a new control before implementation is to ensure that risk is mitigated by the control. A control is a measure or action that is taken to reduce the likelihood or impact of a risk, or to increase the likelihood or impact of an opportunity1. Testing the effectiveness of anew control before implementation means verifying whether the control can achieve its intended purpose and objective, and whether it can address the risk adequately and appropriately2. Testing the effectiveness of a new control before implementation helps to avoid wasting resources, time, and effort on implementing a control that is ineffective, inefficient, or unsuitable for the risk scenario. It also helps to ensure that the control does not introduce new or unintended risks, or adversely affect other controls or processes3. The other options are not the primary objective of testing the effectiveness of a new control before implementation, as they are either less relevant or less specific than ensuring that risk is mitigated by the control. Measuring efficiency of the control process is a secondary objective of testing the effectiveness of a new control before implementation. Efficiency refers to the optimal use of resources to achieve the desired outcome4. Measuring efficiency of the control process means evaluating whether the control can achieve its objective with the least amount of cost, time, and effort. Measuring efficiency of the control process helps to optimize the performance and value of the control, but it is not the main reason for testing the effectiveness of a new control before implementation. Confirming control alignment with business objectives is a tertiary objective of testing the effectiveness of a new control before implementation. Alignment refers to the consistency and coherence of the control with the goals and strategies of the organization5. Confirming control alignment with business objectives means ensuring that the control supports and enables the achievement of the organization' s mission, vision, and values. Confirming control alignment with business objectives helps to integrate the control with the organization's culture and governance, but it is not the primary reason for testing the effectiveness of a new control before implementation. Complying with the organization's policy is a quaternary objective of testing the effectiveness of a new control before implementation. Policy refers to the set of principles and rules that guide the organization's decisions and actions6. Complying with the organization's policy means adhering to the standards and requirements that the organization has established for implementing and operating controls. Complying with the organization's policy helps to ensure the quality and consistency of the control, but it is not the main objective of testing the effectiveness of a new control before implementation. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.8, Page 61.

NEW QUESTION: 830

Which of the following is the MOST effective way to mitigate identified risk scenarios?

A. Assign ownership of the risk response plan

B. Provide awareness in early detection of risk.

C. Perform periodic audits on identified risk.

D. areas Document the risk tolerance of the organization.

Answer: (SHOW ANSWER)

A risk response plan is a document that outlines the actions to be taken to address the identified risk scenarios. A risk response plan should include the objectives, scope, roles and responsibilities, resources, timelines, and metrics for each risk response. Assigning ownership of the risk response plan is the most effective way to mitigate identified risk scenarios, as it ensures accountability, clarity, and communication among the stakeholders involved in the risk management process. Assigning ownership also helps to monitor and evaluate the progress and effectiveness of the risk response plan, and to make adjustments as needed. References = Risk and Information Systems Control Study Manual, Chapter 3: Risk Response and Mitigation, Section 3.3: Risk Response Plan, p. 152-155.

NEW QUESTION: 831
Which of the following is the PRIMARY reason for a risk practitioner to report changes and trends in the IT risk profile to senior management?
A. To ensure risk owners understand their responsibilities
B. To ensure IT risk is managed within acceptable limits
C. To ensure the organization complies with legal requirements
D. To ensure the IT risk awareness program is effective
Answer: (SHOW ANSWER)
The primary reason for a risk practitioner to report changes and trends in the IT risk profile to senior management is to ensure that IT risk is managed within acceptable limits, because it helps to inform and advise the senior management on the current state and direction of IT risk, and to support the risk-based decision making and prioritization. An IT risk profile is a summary of the key IT risks that an organization faces, and their implications for the organization's objectives and strategy. An IT risk profile may change or evolve over time, due to factors such as new technologies, business initiatives, or external events. Reporting changes and trends in the IT risk profile to senior management is the primary reason, as it helps to ensure that the senior management is aware of and prepared for the IT risk challenges and opportunities, and that the IT risk is managed within the acceptable limits defined by the organization's risk appetite and tolerance. To ensure risk owners understand their responsibilities, to ensure the organization complies with legal requirements, and to ensure the IT risk awareness program is effective are all possible reasons for reporting changes and trends in the IT risk profile, but they are not the primary reason, as they are not directly related to the management of IT risk within acceptable limits. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.2.3, page 91

NEW QUESTION: 832
What is the BEST information to present to business control owners when justifying costs related to controls?
A. Loss event frequency and magnitude
B. The previous year's budget and actuals
C. Industry benchmarks and standards
D. Return on IT security-related investments
Answer: (SHOW ANSWER)
The best information to present to business control owners when justifying costs related to controls is the return on IT security-related investments, because this shows the value and benefits of the controls in

relation to their costs. Return on IT security-related investments is a metric that measures the effectiveness and efficiency of IT security controls by comparing the amount of money saved or gained from preventing or mitigating IT-related risks with the amount of money spent on implementing and maintaining the controls. By presenting this information, business control owners can see how the controls contribute to the achievement of the business objectives, such as reducing losses, increasing revenues, enhancing customer satisfaction, or improving compliance. This information can also help business control owners to prioritize and allocate resources for the most critical and beneficial controls, and to optimize the balance between risk and return. References = Cost Control: How Businesses Use It to Increase Profits

NEW QUESTION: 833
Which of the following provides the MOST useful information when determining if a specific control should be implemented?
A. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Attribute analysis
D. Root cause analysis
Answer: (SHOW ANSWER)
A cost-benefit analysis is a tool that compares the costs and benefits of different alternatives, such as implementing or not implementing a specific control. A cost-benefit analysis provides the most useful information when determining if a specific control should be implemented, as it can show the potential savings, benefits, and risks of each option, and help the decision-makers choose the best course of action. A cost-benefit analysis can also include qualitative factors, such as security, compliance, performance, and customer satisfaction, that may be affected by the control implementation. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, Question 256. CRISC: Certified in Risk & Information Systems Control Sample Questions, Question 256. Most Asked CRISC Exam Questions and Answers, Question 10. CRISC by Isaca Actual Free Exam Q&As, Question 9.

NEW QUESTION: 834
An organization's IT department wants to complete a proof of concept (POC) for a security tool. The project lead has asked for approval to use the production data for testing purposes as it will yield the best results. Which of the following is the risk practitioner's BEST recommendation?
A. Accept the risk of using the production data to ensure accurate results.
B. Assess the risk of using production data for testing before making a decision.
C. Benchmark against what peer organizations are doing with POC testing environments.
D. Deny the request, as production data should not be used for testing purposes.
Answer: (SHOW ANSWER)
Assessing the risk of using production data for testing before making a decision is the best recommendation for the risk practitioner, because it helps to balance the benefits and drawbacks of using real data for the proof of concept (POC) of a security tool. A POC is a demonstration or trial of a proposed solution or product to verify its feasibility, functionality, and value. A security tool is a software or hardware device that helps to protect the IT systems or networks from threats or attacks. Using production data for testing purposes can

yield the best results, as it reflects the actual data that the security tool will handle in the operational environment. However, using production data for testing also poses risks, such as data leakage, data corruption, data privacy violation, or regulatory non-compliance. Therefore, assessing the risk of using production data for testing before making a decision is the best recommendation, as it helps to identify and evaluate the potential risks and issues, and to determine the appropriate controls or mitigating factors to reduce or eliminate them. Accepting the risk of using the production data, benchmarking against what peer organizations are doing, and denying the request are all possible recommendations, but they are not the best recommendation, as they do not consider the risk assessment process and the trade-offs involved in using production data for testing. References = Risk and Information Systems Control Study Manual, Chapter 5, Section 5.4.1, page 208

NEW QUESTION: 835
Which of the following has the GREATEST influence on an organization's risk appetite?
A. Threats and vulnerabilities
B. Internal and external risk factors
C. Business objectives and strategies
D. Management culture and behavior
Answer: (SHOW ANSWER)
Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk appetite is influenced by various factors, such as the organization's mission, vision, values, culture, stakeholders, resources, capabilities, etc. However, the factor that has the greatest influence on the organization's risk appetite is the business objectives and strategies, which are the desired outcomes and the plans to achieve them. The business objectives and strategies define the direction and scope of the organization, and the risk appetite reflects the level of risk that the organization is prepared to take to accomplish them. The risk appetite should be aligned with the business objectives and strategies, and should provide guidance for the risk management activities and decisions. References = CRISC Review Manual, 7th Edition, page 61.

NEW QUESTION: 836
An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:
A. avoided.
B. accepted.
C. mitigated.
D. transferred.
Answer: (SHOW ANSWER)
Risk acceptance is a risk response strategy that involves acknowledging the existence and potential impact of a risk, but deciding not to take any action to reduce or eliminate it. Risk acceptance can be appropriate when the cost or effort of implementing a risk response outweighs the benefit, or when there are no feasible or effective risk responses available. An organization has identified that terminated employee accounts are

not disabled or deleted within the time required by corporate policy, which poses a security risk to the organization. The organization is unsure of the reason for this issue, and has decided to monitor the situation for three months to obtain more information, rather than taking any immediate action to resolve the issue. As a result of this decision, the risk has been accepted, as the organization has chosen to tolerate the risk exposure for a certain period of time, and has not implemented any controls or measures to prevent or reduce the risk occurrence or impact. References = Risk Response Strategies: Avoid, Transfer, Mitigate, Accept, Risk Response Strategies: What They Are and How to Use Them, Risk Response Strategy: Definition, Types, and Examples.

NEW QUESTION: 837
Which of the following is MOST important when developing risk scenarios?
A. Reviewing business impact analysis (BIA)
B. Collaborating with IT audit
C. Conducting vulnerability assessments
D. Obtaining input from key stakeholders
Answer: (SHOW ANSWER)
The most important factor when developing risk scenarios is obtaining input from key stakeholders. A risk scenario is a description of a possible event or situation that could affect the enterprise's objectives, processes, or resources. Obtaining input from key stakeholders, such as business owners, process owners, subject matter experts, or external parties, helps to ensure that the risk scenarios are realistic, relevant, and comprehensive. It also helps to identify the sources, drivers, indicators, likelihood, impact, and responses of the risk scenarios, and to align them with the enterprise's risk appetite and tolerance. Obtaining input from key stakeholders also fosters a collaborative and participatory approach to risk management, and enhances the risk awareness and ownership among the stakeholders. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section 2.1.3, page 621

NEW QUESTION: 838
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?
A. Ensuring that database changes are correctly applied
B. Enforcing that changes are authorized
C. Deterring illicit actions of database administrators
D. Preventing system developers from accessing production data
Answer: (SHOW ANSWER)
Ensuring that database changes are correctly applied is the primary reason for monitoring activities performed in a production database environment, as it helps to maintain the integrity, availability, and performance of the database and the applications that depend on it. Database changes are any modifications made to the database structure, configuration, data, or code, such as adding or deleting tables, columns, indexes, or triggers, updating or inserting data, or altering stored procedures or functions. Database changes can have significant impacts on the database functionality and behavior, and may introduce errors, inconsistencies, or vulnerabilities if not applied correctly. Therefore, monitoring database changes is

essential to verify that the changes are implemented as intended, comply with the design specifications and standards, and do not cause any adverse effects or conflicts with the existing database or application components.
The other options are not the primary reasons for monitoring activities performed in a production database environment. Enforcing that changes are authorized is an important aspect of database change management, but it is not the main purpose of database monitoring. Database change management is the process of planning, reviewing, approving, and implementing database changes in a controlled and consistent manner.
Database change management helps to ensure that the changes are authorized by the appropriate stakeholders, aligned with the business requirements and objectives, and documented and communicated to the relevant parties. Database monitoring can support database change management by providing information and feedback on the change implementation and performance, but it does not enforce the change authorization.
Deterring illicit actions of database administrators is a possible benefit of database monitoring, but it is not the primary reason for it. Database administrators are the users who have the highest level of access and privilege to the database, and they are responsible for managing and maintaining the database operations and security.
Database monitoring can help to deter illicit actions of database administrators by tracking and auditing their activities and actions on the database, and alerting or escalating any suspicious or malicious behavior. However, database monitoring is not the only or the most effective way to prevent or detect illicit actions of database administrators. Other measures, such as implementing the principle of least privilege, segregating duties, enforcing password policies, and encrypting data, are also necessary to protect the database from unauthorized or improper access or manipulation by database administrators or other users. Preventing system developers from accessing production data is a possible benefit of database monitoring, but it is not the primary reason for it. System developers are the users who design, develop, and test the applications that interact with the database. System developers should not have access to the production data, as it may contain sensitive or confidential information that could be compromised or misused by the developers. System developers should only use test or dummy data for their development and testing purposes.
Database monitoring can help to prevent system developers from accessing production data by controlling and restricting their access and privilege to the database, and logging and reporting any unauthorized or inappropriate access attempts. However, database monitoring is not the only or the most effective way to prevent system developers from accessing production data. Other measures, such as implementing access control policies, masking or anonymizing data, and isolating development and production environments, are also necessary to safeguard the production data from system developers or other users. References = Database Monitoring: Basics & Introduction | Splunk, IT Risk Resources | ISACA, Best Practices for Database Performance Monitoring

NEW QUESTION: 839
Which of the following refers to the maximum level of risk an organization is able to bear in order to achieve its objectives?
A. Risk tolerance

B. Risk velocity
C. Risk appetite
D. Risk capacity
Answer: D (LEAVE A REPLY)
Risk capacity refers to the maximum level of risk an organization can absorb or sustain without jeopardizing its viability. It is directly influenced by the organization's financial resources and largest annualized losses it can bear. Risk appetite and risk tolerance reflect willingness and acceptable variations but are distinct from capacity, which is the hard limit on risk exposure.

NEW QUESTION: 840
The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:
Freecram.net
A. changes due to emergencies.
B. changes that cause incidents.
C. changes not requiring user acceptance testing.
D. personnel that have rights to make changes in production.
Answer: (SHOW ANSWER)
Changes deployed to production are those that affect the functionality, performance, or security of the system in a way that is visible or accessible to the end users1. These changes can introduce new risks or vulnerabilities, such as errors, bugs, compatibility issues, or unauthorized access2. Therefore, it is important to monitor the risk associated with these changes and measure how often they cause incidents in production. One metric that can be used to monitor this risk is the percentage of changes that cause incidents in production. This metric indicates how effective the change management process is and how well the organization can prevent or mitigate potential problems caused by changes3. A high percentage of incidents indicates a high level of risk and a need for improvement in the change management process.
References = IT Change Management for SOC: Process and Best Practices, Determining and Managing Risk when Deploying Code, 6 Deployment Risks and How To Mitigate Them

NEW QUESTION: 841
Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?
A. It provides a cost-benefit analysis on control options available for implementation.
B. It provides a view on where controls should be applied to maximize the uptime of servers.
C. It provides historical information about the impact of individual servers malfunctioning.
D. It provides a comprehensive view of the impact should the servers simultaneously fail.
Answer: (SHOW ANSWER)
Using an entry in the risk register to track the aggregate risk associated with server failure provides a comprehensive view of the impact should the servers simultaneously fail, as it considers the combined effect of the server failure on the enterprise's objectives and operations. The risk register is a document that records and tracks the identified risks, their likelihood, impact, and mitigation strategies. By aggregating the risk associated with server failure, the risk register can help to estimate the worst-case scenario and to

prioritize the risk response accordingly. It provides a cost-benefit analysis on control options available for implementation, it provides a view on where controls should be applied to maximize the uptime of servers, and it provides historical information about the impact of individual servers malfunctioning are not the primary benefits of using an entry in the risk register to track the aggregate risk associated with server failure, but rather the possible outcomes or actions of using the risk register. References = CRISC Certified in Risk and Information Systems Control - Question220; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 220.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 842
An organization's capability to implement a risk management framework is PRIMARILY influenced by the:
A. guidance of the risk practitioner.
B. competence of the staff involved.
C. approval of senior management.
D. maturity of its risk culture.
Answer: (SHOW ANSWER)
The factor that primarily influences an organization's capability to implement a risk management framework is the maturity of its risk culture, as it reflects the degree of awareness, understanding, and commitment of the organization's stakeholders towards the risk management objectives, values, and practices, and affects the adoption and integration of the risk management framework across the organization. The other options are not the primary factors, as they are more related to the guidance, competence, or approval of the risk management framework, respectively, rather than the influence of the risk management framework. References = CRISC Review Manual, 7th Edition, page 99.

NEW QUESTION: 843
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager.
Which of the following would be the BEST method to use when developing the scenarios?
A. Cause-and-effect diagram
B. Delphi technique
C. Bottom-up approach
D. Top-down approach
Answer: (SHOW ANSWER)

A cause-and-effect diagram, also known as a fishbone diagram or an Ishikawa diagram, is a graphical tool that helps to identify and analyze the potential causes and effects of a problem or an event. A cause-and-effect diagram can be used to develop technical risk scenarios related to a recently developed ERP system, because it can help to:
Break down the complex problem or event into manageable and measurable categories and subcategories of causes and effects Visualize the relationships and interactions among the various factors that contribute to the problem or event Identify the root causes and the most significant effects of the problem or event Generate ideas and hypotheses for testing and validating the problem or event Communicate and present the problem or event clearly and logically to the stakeholders1 A cause-and-effect diagram can be constructed by following these steps:
Define the problem or event and write it in a box on the right side of the diagram Draw a horizontal line from the box to the left side of the diagram, representing the main spine of the fishbone Identify the major categories of causes that affect the problem or event, such as people, process, technology, environment, etc., and write them on the branches of the spine For each category, brainstorm and list the possible subcategories and specific causes that influence the problem or event, and write them on the sub-branches of the spine For each cause, identify and list the possible effects or consequences that result from the problem or event, and write them on the sub-sub-branches of the spine Analyze the diagram and prioritize the causes and effects based on their frequency, severity, and controllability Develop technical risk scenarios based on the most critical causes and effects, and describe how they could affect the ERP system and the organization1

NEW QUESTION: 844
In which of the following system development life cycle (SDLC) phases should controls be incorporated into system specifications?
A. Implementation
B. Development
C. Design
D. Feasibility
Answer: (SHOW ANSWER)
Controls should be incorporated into system specifications in the design phase of the system development life cycle (SDLC), because this is the phase where the system requirements are translated into detailed specifications and architectures that define how the system will be built and operated. Incorporating controls in the design phase ensures that the system is secure, reliable, and compliant from the start, and reduces the cost and complexity of implementing controls later in the SDLC. The other options are not the correct answers, because they are not the phases where controls are incorporated into system specifications. The implementation phase is the phase where the system is installed, configured, and tested. The development phase is the phase where the system is coded, integrated, and tested. The feasibility phase is the phase where the system concept and scope are defined and evaluated. References = CRISC: Certified in Risk & Information Systems Control Sample Questions

NEW QUESTION: 845

Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

A. Time required for backup restoration testing

B. Change in size of data backed up

C. Successful completion of backup operations

D. Percentage of failed restore tests

Answer: (SHOW ANSWER)

The most appropriate key risk indicator (KRI) for backup media that is recycled monthly is the percentage of failed restore tests. A KRI is a metric that measures the likelihood or impact of a risk, and provides an early warning signal of a potential risk event. The percentage of failed restore tests is a KRI that reflects the quality and reliability of the backup media, and indicates the possibility of data loss or corruption. A high percentage of failed restore tests would suggest that the backup media is not functioning properly, and that the risk of data unavailability is increasing. Therefore, this KRI would help the risk practitioner to monitor the risk and take corrective actions as needed. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 5, Section 5.2.2, page 235.

NEW QUESTION: 846

Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance

B. Risk appetite

C. Risk awareness

D. Risk policy

Answer: (SHOW ANSWER)

According to the CRISC Review Manual1, risk tolerance is the acceptable level of variation that management is willing to allow for any particular risk as it pursues its objectives. Risk tolerance provides a helpful reference point when communicating the results of a risk assessment to stakeholders, as it helps to compare the current level of risk exposure with the desired level of risk exposure, and to prioritize and allocate resources for risk response. Risk tolerance also helps to align the risk assessment results with the stakeholder expectations and preferences, and to facilitate risk-based decision making. References = CRISC Review Manual1, page 192.

NEW QUESTION: 847

Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

A. To support decision-making for risk response

B. To hold risk owners accountable for risk action plans

C. To secure resourcing for risk treatment efforts

D. To enable senior management to compile a risk profile

Answer: (SHOW ANSWER)

The primary reason for sharing risk assessment reports with senior stakeholders is to support decision-making for risk response. Risk assessment reports are documents that summarize the results of the risk

assessment process, such as the risk sources, causes, impacts, likelihood, and levels. Risk assessment reports also provide recommendations for risk response options, such as avoiding, reducing, transferring, or accepting the risk.
Sharing risk assessment reports with senior stakeholders helps to inform them of the current risk situation, and to solicit their input, feedback, or approval for the risk response actions. The other options are not the primary reason for sharing risk assessment reports, although they may be secondary reasons or outcomes.
References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 4-13.

NEW QUESTION: 848
A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?
A. The business owner
B. The ERP administrator
C. The project steering committee
D. The IT project manager
Answer: (SHOW ANSWER)
The business owner should own the risk if the ERP and payroll system fail to operate as expected, because the business owner is ultimately responsible for the business processes and objectives that depend on the systems.
The other options are not the risk owners, because:
* Option B: The ERP administrator is responsible for the technical aspects of the ERP system, but not the payroll system or the business outcomes.
* Option C: The project steering committee is responsible for overseeing the project of replacing the ERP system, but not the ongoing operation and maintenance of the systems or the business risks.
* Option D: The IT project manager is responsible for managing the project of replacing the ERP system, but not the payroll system or the business risks. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 90.

NEW QUESTION: 849
How should an organization approach the retention of data that is no longer needed for business operations?
A. Data should be retained for a reasonable period of time in case of system rollback.
B. Data should be destroyed or retained on the basis of a cost-benefit analysis.
C. Data should be retained based on regulatory requirements.
D. Data should be destroyed to avoid any risk exposure.
Answer: C (LEAVE A REPLY)
Regulatory and legal compliance dictate data retention requirements, making them the primary basis for retention decisions.
Reference:CRISC Manual - Domain 1, Slide 462, 560

NEW QUESTION: 850

Which of the following is the BEST way to maintain a current list of organizational risk scenarios?

A. Automate workflow for risk status updates.

B. Perform regular reviews of key controls.

C. Conduct periodic risk reviews with stakeholders.

D. Conduct compliance reviews.

Answer: (SHOW ANSWER)

Regular reviews with stakeholders ensure the risk scenarios are current, complete, and relevant.

Stakeholders provide operational and strategic insights, enabling the identification of new, evolving, or obsolete risks.

Periodic reviews foster dynamic and continuous alignment of risk scenarios with the business context and threat landscape.

Reference:CRISC Manual - Domain 2, Slide 256, 210

NEW QUESTION: 851

An organization has restructured its business processes, and the business continuity plan (BCP) needs to be revised accordingly. Which of the following should be identified FIRST?

A. Variances in recovery times

B. Ownership assignment for controls

C. New potentially disruptive scenarios

D. Contractual changes with customers

Answer: (SHOW ANSWER)

When an organization restructures its business processes, the first step in revising the BCP is to identify new potentially disruptive scenarios that may affect the continuity of the critical functions and processes. This can be done by conducting a risk assessment or a business impact analysis (BIA) to determine the likelihood and impact of various threats and vulnerabilities on the organization's objectives and operations. By identifying new potentially disruptive scenarios, the organization can then update its recovery strategies, objectives, and plans accordingly.

References:

*ISACA, Risk IT Framework, 2nd Edition, 2019, p. 761

*ISACA, IT Business Continuity/Disaster Recovery Audit Program, 2021, p. 52

NEW QUESTION: 852

An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

A. Transfer

B. Mitigation

C. Avoidance

D. Acceptance

Answer: (SHOW ANSWER)

Risk avoidance is a type of risk response that involves eliminating the risk entirely by not engaging in the activity that causes the risk or changing the conditions that create the risk1. Risk avoidance is usually applied when the potential impact or likelihood of the risk is high or unacceptable, and when the benefits of avoiding the risk outweigh the costs or losses of doing so2.
In this case, the organization has adopted risk avoidance as its risk response, because it has decided to postpone the decision that could trigger the risk. By delaying the decision, the organization is avoiding the risk of making a wrong or unfavorable choice among the multiple options. However, this may not be the best or most effective risk response, as it could also result in missed opportunities, wasted resources, or increased uncertainty3. The organization should consider the trade-offs and consequences of avoiding the risk, and explore other possible risk responses that could reduce or transfer the risk.
The other options are not the risk responses that the organization has adopted. Risk transfer means shifting the responsibility or burden of the risk to another party, such as a vendor or an insurer2. The organization has not transferred the risk to anyone else, but rather avoided it by postponing the decision. Risk mitigation means implementing controls or safeguards to minimize the negative effects of the risk2. The organization has not mitigated the risk by reducing its impact or likelihood, but rather avoided it by delaying the decision. Risk acceptance means acknowledging the risk and its consequences without taking any action to address it2. The organization has not accepted the risk by tolerating its potential outcomes, but rather avoided it by postponing the decision. References =
* 10 Risk Mitigation techniques you need to know - Stakeholdermap.com
* Risk Response Strategies: Types & Examples (+ Free Template)
* [CRISC Review Manual, 7th Edition]

NEW QUESTION: 853
An organization has identified the need to implement an asset tiering model to establish the appropriate level of impact. Which of the following is the MOST effective risk assessment methodology for a risk practitioner to use for this initiative?
A. Qualitative method
B. Industry calibration method
C. Threat-based method
D. Quantitative method
Answer: (SHOW ANSWER)
Implementing an asset tiering model to establish the appropriate level of impact is best served by a quantitative risk assessment methodology. This approach provides a numeric value to the risk levels, which is crucial for accurately tiering assets.
Quantitative Risk Assessment:
Numeric Values:Quantitative methods assign numerical values to the probability and impact of risks, which allows for precise calculations of risk levels. This precision is essential when establishing tiers for assets based on their impact levels.
Data-Driven Decisions:These methods use statistical data and models to predict potential losses and the probability of various risk events, leading to more informed decision-making.
Asset Tiering Model:

Impact Assessment:Quantitative methods allow for detailed impact assessments. By using numeric values, it is easier to compare the potential impacts of different assets and categorize them into appropriate tiers.
Resource Allocation:Precise risk calculations help in the effective allocation of resources. Higher-tier assets (those with higher impact) can be allocated more resources for protection.
References:
According to the CRISC Review Manual, quantitative risk assessment methods are suitable for situations requiring precise impact assessments and detailed analysis, as they provide a clear, numeric representation of risks.

NEW QUESTION: 854
Which of the following will BEST help to ensure implementation of corrective action plans?
A. Establishing employee awareness training
B. Assigning accountability to risk owners
C. Selling target dates to complete actions
D. Contracting to third parties
Answer: (SHOW ANSWER)
The best way to ensure the implementation of corrective action plans is to assign accountability to risk owners. Corrective action plans are the plans that describe the actions and resources that are needed to correct or improve the performance or compliance of the processes or controls. Risk owners are the persons who have the authority and responsibility for managing the risks and their responses. By assigning accountability to risk owners, the implementation of corrective action plans can be monitored, evaluated, and enforced, and the results and outcomes can be reported and communicated. The other options are not as effective as assigning accountability to risk owners, as they are related to the training, scheduling, or outsourcing of the corrective action plans, not the oversight or governance of the corrective action plans.
References = Risk and Information Systems Control Study Manual, Chapter 4: Risk and Control Monitoring and Reporting, Section
4.4: Key Control Indicators, page 211.

NEW QUESTION: 855
Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?
A. User provisioning
B. Role-based access controls
C. Security log monitoring
D. Entitlement reviews
Answer: (SHOW ANSWER)
An organization's account provisioning process is the process of creating, modifying, or deleting user accounts and access rights for the organization's information systems and resources. It involves defining the access requirements, policies, and standards, and implementing and enforcing them across the organization. The best evidence of the effectiveness of an organization's account provisioning process is entitlement reviews, which are the periodic or regular reviews and validations of the user accounts and access rights that

are granted or assigned to the users or entities that interact with the organization's information systems and resources. Entitlement reviews can provide assurance and verification that the account provisioning process is accurate, consistent, and compliant, and that it meets the organization's security and business objectives and requirements.
Entitlement reviews can be performed using various techniques, such as automated tools, reports, audits, surveys, etc. Entitlement reviews can also be integrated with the organization's governance, risk management, and compliance functions, and aligned with the organization's policies and standards.
The other options are not the best evidence of the effectiveness of an organization's account provisioning process, because they do not provide the same level of assurance and verification that the account provisioning process is accurate, consistent, and compliant, and that it meets the organization's security and business objectives and requirements.
User provisioning is the process of creating, modifying, or deleting user accounts and access rights for a specific user or entity, based on their identity, role, or function in the organization. User provisioning is an important part of the account provisioning process, but it is not the best evidence of the effectiveness of the account provisioning process, because it does not indicate whether the user accounts and access rights are appropriate and authorized, and whether they comply with the organization's policies and standards.
Role-based access controls are the controls that grant or restrict user accounts and access rights based on the predefined roles or functions that the users or entities perform or assume in the organization. Role-based access controls are an important part of the account provisioningprocess, but they are not the best evidence of the effectiveness of the account provisioning process, because they do not indicate whether the roles or functions are defined and assigned correctly and consistently, and whether they comply with the organization' s policies and standards.
Security log monitoring is the process of collecting, analyzing, and reporting on the security events or activities that are recorded or logged by the organization's information systems and resources. Security log monitoring is an important part of the account provisioning process, but it is not the best evidence of the effectiveness of the account provisioning process, because it does not indicate whether the security events or activities are legitimate or authorized, and whether they comply with the organization's policies and standards. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 40-41, 47-48, 54-55, 58-59, 62-63 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 173 CRISC Practice Quiz and Exam Prep

NEW QUESTION: 856
A multinational company needs to implement a new centralized security system. The risk practitioner has identified a conflict between the organization's data-handling policy and local privacy regulations. Which of the following would be the BEST recommendation?
A. Report the noncompliance to the local regulatory agency.
B. Comply with the organizational policy.
C. Request an exception from the local regulatory agency.
D. Request a policy exception from senior management.
Answer: (SHOW ANSWER)

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 857
Which of the following is the MOST important data attribute of key risk indicators (KRIs)?
A. The data is measurable.
B. The data is calculated continuously.
C. The data is relevant.
D. The data is automatically produced.
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are metrics that provide information about the level of exposure to a specific risk or a group of risks.
The most important data attribute of KRIs is that the data is relevant. This means that the data reflects the current state of the risk, the potential impact of the risk, and the effectiveness of the risk response. Relevant data helps to monitor and measure the risk performance and to make informed decisions about risk management.
The other options are not the most important data attributes of KRIs. They are either secondary or not essential for KRIs.
The references for this answer are:
Risk IT Framework, page 15
Information Technology & Security, page 9
Risk Scenarios Starter Pack, page 7

NEW QUESTION: 858
Which of the following should be the PRIMARY input when designing IT controls?
A. Benchmark of industry standards
B. Internal and external risk reports
C. Recommendations from IT risk experts
D. Outcome of control self-assessments
Answer: (SHOW ANSWER)
The primary input when designing IT controls should be internal and external risk reports. IT controls are specific activities performed by persons or systems to ensure that business objectives are met, and thatthe confidentiality, integrity, and availability of data and the overall management of the IT function are ensured1. Designing IT controls means creating and implementing the appropriate measures or actions to reduce the likelihood or impact of the IT risks that may affect the organization2. Internal and external risk reports are documents that provide information and analysis on the current and potential IT risks that the organization

faces, as well as their sources, drivers, consequences, and responses3. Internal risk reports are generated by the organization itself, such as by the IT risk management function, the internal audit function, or the business units. External risk reports are obtained from external sources, such as regulators, industry associations, or third-party service providers. Internal and external risk reports are the primary input when designing IT controls, because they help to:
Identify and prioritize the IT risks that need to be addressed by the IT controls; Evaluate the likelihood and impact of the IT risks, and compare them against the organization's risk appetite and tolerance; Determine the most suitable and effective IT control objectives and activities to mitigate the IT risks; Align the IT control design and implementation with the organization's objectives, strategies, and values; Monitor and measure the performance and effectiveness of the IT controls in reducing the IT risks. The other options are not the primary input when designing IT controls, as they are either less relevant or less specific than internal and external risk reports. Benchmark of industry standards is a comparison of the organization's IT control practices and performance with those of other organizations in the same industry or sector4.
Benchmark of industry standards can help to improve the quality and consistency of the IT control design and implementation, as well as to identify the best practices and gaps. However, benchmark of industry standards is not the primary input when designing IT controls, as it does not address the specific IT risks that the organization faces, or the IT control objectives and activities that are appropriate and effective for the organization. Recommendations from IT risk experts are the suggestions or advice from the professionals or specialists who have the knowledge and experience in IT risk management and IT control design and implementation5. Recommendations from IT risk experts can help to enhance the IT control design and implementation, as well as to provide guidance and support to the organization. However, recommendations from IT risk experts are not the primary input when designing IT controls, as they are based on the opinions and perceptions of the experts, and may not reflect the actual or objective level and nature of the IT risks, or the IT control objectives and activities that are suitable and efficient for the organization. Outcome of control self-assessments is the result or conclusion of the evaluation and testing of the design and operation of the existing IT controls by the organization itself, such as by the IT control owners, the IT risk management function, or the business units6. Outcome of control self-assessments can help to improve the IT control design and implementation, as well as to detect and correct any issues or deficiencies. However, outcome of control self-assessments is not the primary input when designing IT controls, as it does not cover the new or emerging IT risks that the organization may face, or the IT control objectives and activities that are relevant and necessary for the organization. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.1, Page 189.

NEW QUESTION: 859
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:
A. risk appetite.
B. security policies
C. process maps.
D. risk tolerance level
Answer: (SHOW ANSWER)

When collecting information to identify IT-related risk, a risk practitioner should first focus on IT risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its IT objectives, before action is deemed necessary to reduce the risk1. IT risk appetite reflects the organization's IT risk attitude and its willingness to accept risk in specific scenarios, with a governance model in place for IT risk oversight. IT risk appetite helps to guide the organization's approach to IT risk and IT risk management, and to align its IT risk decisions with its business objectives and context. The other options are not the best answers, as they are either derived from or dependent on the IT risk appetite. IT security policies are the rules and guidelines that define the organization's IT security objectives, requirements, and responsibilities, and they are based on the IT risk appetite. IT process maps are the graphical representations of the IT processes, activities, and tasks that support the organization's IT objectives, and they are influenced by the IT risk appetite. IT risk tolerance level is the acceptable variation between the IT risk thresholds and the IT objectives, and it is determined by the IT risk appetite. References = IT Risk Resources | ISACA; Risk Appetite vs. Risk Tolerance: What is the Difference?; IT Risk Management - an overview | ScienceDirect Topics; IT Risk Management Framework - an overview | ScienceDirect Topics

NEW QUESTION: 860

Which of the following is the GREATEST risk of relying on artificial intelligence (AI) within heuristic security systems?

Freecram.net

A. AI may result in less reliance on human intervention.
B. Malicious activity may inadvertently be classified as normal during baselining.
C. Risk assessments of heuristic security systems are more difficult.
D. Predefined patterns of malicious activity may quickly become outdated.
Answer: (SHOW ANSWER)
AI in Heuristic Security Systems:
* Heuristic security systems use artificial intelligence (AI) to identify and respond to potential threats by learning from data patterns and behaviors.
Risk of Misclassification:
* During the baselining process, AI systems establish what is considered normal behavior. If malicious activity is present during this period, it may be incorrectly classified as normal.
* This misclassification can lead to undetected security breaches, as the system will not recognize these activities as threats in the future.
Impact of Misclassification:
* Misclassified malicious activities can lead to significant security risks, allowing attackers to operate undetected within the system.
* It undermines the effectiveness of the heuristic system, reducing its ability to protect the organization from real threats.
Comparing Other Risks:
* Less Reliance on Human Intervention: This is a general concern but does not directly impact the accuracy of threat detection.
* Difficulty in Risk Assessments: While a challenge, it is not the greatest risk compared to misclassification of malicious activity.

* Outdated Patterns: While a concern, the primary risk lies in initial misclassification during baselining.
References:
* The CRISC Review Manual discusses the challenges of AI in security systems, particularly the risk of misclassification during the learning phase (CRISC Review Manual, Chapter 4: Information Technology and Security, Section 4.7.4 Artificial Intelligence) .

NEW QUESTION: 861
Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?
A. Use an encrypted tunnel lo connect to the cloud.
B. Encrypt the data in the cloud database.
C. Encrypt physical hard drives within the cloud.
D. Encrypt data before it leaves the organization.
Answer: D (LEAVE A REPLY)
Encrypting data before it leaves the organization is the best way to protect sensitive data from administrators within a public cloud, as it ensures that the data is secured at the source and remains encrypted throughout the transmission and storage in the cloud. Using an encrypted tunnel to connect to the cloud, encrypting the data in the cloud database, and encrypting physical hard drives within the cloud are not the best ways, as they may not prevent the cloud administrators from accessing the data or the encryption keys, or may not protect the data from unauthorized interception or modification during the transmission. References = CRISC Review Manual, 7th Edition, page 153.

NEW QUESTION: 862
An organization's risk tolerance should be defined and approved by which of the following?
A. The chief risk officer (CRO)
B. The board of directors
C. The chief executive officer (CEO)
D. The chief information officer (CIO)
Answer: (SHOW ANSWER)
The organization's risk tolerance should be defined and approved by the board of directors, as they are the highest governing body of the organization and have the ultimate responsibility and accountability for the strategic direction and oversight of the risk management process. The board of directors should establish and communicate the risk appetite and tolerance of the organization, and ensure that they are aligned with the organization's vision, mission, values, and goals. The board of directors should also monitor and review the risk management performance and outcomes, and provide guidance and support to the management and staff.
The other options are not the correct answers, as they do not have the authority or responsibility to define and approve the organization's risk tolerance, although they may have some roles or involvement in the risk management process. The chief risk officer (CRO) is the senior executive who leads and coordinates the risk management activities across the organization, and reports to the board of directors and the chief executive officer (CEO). The CRO should advise and assist the board of directors in defining and approving the risk tolerance, but they cannot do it on their own. The chief executive officer (CEO) is the highest-ranking

manager of the organization and has the responsibility and accountability for the execution and implementation of the risk management process. The CEO should support and communicate the risk tolerance defined and approved by the board of directors, but they cannot do it on their own. The chief information officer (CIO) is the senior executive who oversees and manages the information and technology functions and resources of the organization. The CIO should ensure that the IT risks and controls are aligned with the risk tolerance defined and approved by the board of directors, but they cannot do it on their own. References = Risk and Information Systems Control Study Manual, Chapter 1: IT Risk Identification, page 24.

NEW QUESTION: 863
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?
A. Increase in compliance breaches
B. Increase in loss event impact
C. Increase in residual risk
D. Increase in customer complaints
Answer: (SHOW ANSWER)
A loss event is an occurrence that results in a negative consequence or damage for an organization, such as a data breach, a cyberattack, or a natural disaster. The impact of a loss event is the extent or magnitude of the harm or loss caused by the event, such as financial losses, reputational damage, operational disruptions, or legal liabilities. A newly enacted information privacy law that significantly increases financial penalties for breaches of personally identifiable information (PII) will most likely increase the impact of a loss event for an organization affected by the new law, because it will increase the potential cost and severity of a data breach involving PII. The other options are not as likely as an increase in loss event impact, because they do not directly result from the new law, but rather depend on other factors, such as the organization's risk management capabilities, as explained below:
* A. Increase in compliance breaches is not a likely outcome, because it assumes that the organization will not comply with the new law, which would expose it to more risks and penalties. A rational organization would try to comply with the new law by implementing appropriate controls and measures to protect PII and prevent data breaches.
* C. Increase in residual risk is not a likely outcome, because it assumes that the organization will not adjust its risk response strategies to account for the new law, which would leave it with more risk exposure than desired. A prudent organization would try to reduce its residual risk by enhancing its risk mitigation controls or transferring its risk to a third party, such as an insurance company.
* D. Increase in customer complaints is not a likely outcome, because it assumes that the organization will experience more data breaches involving PII, which would affect its customer satisfaction and loyalty. A responsible organization would try to avoid data breaches by improving its security posture and practices, and by communicating transparently and effectively with its customers about the new law and its implications. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.1.1, page 32.

NEW QUESTION: 864
An organization's finance team is proposing the adoption of a blockchain technology to provide a secure method for moving funds. Which of the following should the risk practitioner do FIRST?
A. Recommend permissionless blockchain.
B. Perform a risk assessment.
C. Perform a business impact analysis (BIA).
D. Recommend permissioned blockchain.
Answer: (SHOW ANSWER)
Before selecting technologies or deployment models, a risk assessment should be conducted to evaluate potential threats, vulnerabilities, and controls. This ensures the technology aligns with the risk appetite and regulatory requirements of the organization.
Reference:CRISC Manual - Domain 2, Slide 178-180, 250

NEW QUESTION: 865
Which of the following is the BEST way to support communication of emerging risk?
A. Update residual risk levels to reflect the expected risk impact.
B. Adjust inherent risk levels upward.
C. Include it on the next enterprise risk committee agenda.
D. Include it in the risk register for ongoing monitoring.
Answer: (SHOW ANSWER)
Emerging risk is a risk that is new or evolving, and has the potential to significantly affect the enterprise's objectives, performance, or reputation. Emerging risk can arise from changes in the internal or external environment, such as technological innovations, regulatory developments, or social trends. The best way to support communication of emerging risk is to include it on the next enterprise risk committee agenda. The enterprise risk committee is a group of senior executives who oversee the enterprise-wide risk management program, and provide guidance and direction to the risk owners and practitioners. By including the emerging risk on the agenda, the risk practitioner can ensure that the enterprise risk committee is aware of the risk, its causes, impacts, and likelihood, and can decide on the appropriate risk response strategy and actions. The other options are not the best way to support communication of emerging risk, as they involve different aspects of the risk management process:
* Update residual risk levels to reflect the expected risk impact means that the risk practitioner adjusts the risk levels after considering the existing or planned risk responses. This may not be feasible or accurate for emerging risk, as the risk responses may not be defined or implemented yet, or may not be effective for the new or evolving risk.
* Adjust inherent risk levels upward means that the risk practitioner increases the risk levels before considering any risk responses. This may not reflect the true nature or magnitude of the emerging risk, as the inherent risk levels are based on the assumptions and estimates of the risk practitioner, and may not account for the uncertainties or complexities of the emerging risk.
* Include it in the risk register for ongoing monitoring means that the risk practitioner records and tracks the emerging risk, its causes, impacts, likelihood, responses, and owners. This is an important step in the risk

management process, but it does not necessarily support communication of the emerging risk, as the risk register may not be accessible or visible to all the relevant stakeholders, or may not be updated or reviewed frequently enough to capture the changes in the emerging risk. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 1, Section 1.2.2.2, pp. 21-22.

NEW QUESTION: 866
Which of the following should be a risk practitioner's GREATEST concern upon learning of failures in a data migration activity?
A. Availability of test data
B. Integrity of data
C. Cost overruns
D. System performance
Answer: (SHOW ANSWER)
The integrity of data should be the greatest concern for a risk practitioner upon learning of failures in a data migration activity, because it affects the accuracy, completeness, and consistency of the data that are transferred from one system or format to another. Data integrity is a property of data that ensures that the data are valid, reliable, and trustworthy, and that they have not been altered or corrupted by unauthorized or accidental means. Data migration is a process of moving or copying data from one system or format to another, usually as part of a system upgrade, consolidation, or transformation. Data migration can pose risks to the integrity of data, such as data loss, duplication, inconsistency, or corruption, due to factors such as incompatible formats, human errors, technical glitches, or malicious attacks. Therefore, the integrity of data should be the greatest concern, as it impacts the quality and usability of the data, and the performance and functionality of the system. The availability of test data, the cost overruns, and the system performance are all possible concerns for a risk practitioner, but they are not the greatest concern, as they do not directly affect the integrity of data. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

NEW QUESTION: 867
Which of the following should be done FIRST when developing a data protection management plan?
A. Perform a cost-benefit analysis.
B. Identify critical data.
C. Establish a data inventory.
D. Conduct a risk analysis.
Answer: (SHOW ANSWER)
A data protection management plan is a document that outlines how an organization will protect its sensitive data from unauthorized access, use, disclosure, or loss. A data protection management plan should include the following components1:
The scope and objectives of the data protection management plan, and how it aligns with the organization's data protection policy and strategy The roles and responsibilities of the data protection team and other stakeholders, and how they will communicate and coordinate The data protection risks and threats that the organization faces, and how they will be assessed and prioritized The data protection controls and measures

that the organization will implement and maintain, and how they will be monitored and evaluated The data protection incidents and breaches that the organization may encounter, and how they will be reported and resolved The data protection training and awareness programs that the organization will provide and conduct, and how they will be measured and improved The first step that should be done when developing a data protection management plan is to identify critical data. This means that the organization should:
Define what constitutes sensitive data in the organization, such as personal data, confidential data, or regulated data Identify and classify the sensitive data that the organization collects, processes, stores, or transfers, and assign appropriate labels or tags Determine the value and importance of the sensitive data to the organization and its stakeholders, and the potential impacts or consequences of data loss or compromise Map the data flows and locations of the sensitive data within the organization and across its partners or vendors, and document the data lifecycle stages and activities By identifying critical data, the organization can:
Establish a clear and consistent understanding of the data protection scope and objectives, and ensure that they are relevant and realistic Provide a comprehensive and accurate data inventory that can support the data protection risk assessment and control implementation Identify and prioritize the data protection needs and requirements of the organization and its stakeholders, and align them with the data protection laws and standards Communicate and report the data protection status and performance to the stakeholders and regulators, and ensure transparency and accountability References = Guide to Developing a Data Protection Management Programme

NEW QUESTION: 868
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?
A. Review the design of the machine learning model against control objectives.
B. Adopt the machine learning model as a replacement for current manual access reviews.
C. Ensure the model assists in meeting regulatory requirements for access controls.
D. Discourage the use of emerging technologies in key processes.
Answer: (SHOW ANSWER)
The risk practitioner's best course of action is to review the design of the machine learning model against the control objectives, because this will help to evaluate the suitability, effectiveness, and reliability of the model as a control measure. A machine learning model is a type of artificial intelligence that can learn from data and make predictions or decisions based on the data. A machine learning model can be used to automate or enhance the access management process, such as by identifying excessive access privileges, detecting unauthorized access, or recommending access rights. However, a machine learning model also introduces new risks and challenges, such as data quality, model accuracy, model bias, model explainability, model security, and model governance. Therefore, the risk practitioner should review the design of the machine learning model against the control objectives, which are the specific goals or outcomes that the control is intended to achieve. The control objectives can be derived from the IT risk management strategy, the IT governance framework, the IT policies and standards, and the regulatory requirements. The review of the machine learning model should cover the following aspects: - The data sources and inputs: The risk practitioner should verify that the data used to train and test the machine learning model is relevant,

complete, accurate, consistent, and representative of the access management process and the access rights. The risk practitioner should also check that the data is collected, stored, processed, and transmitted in a secure and compliant manner, and that the data privacy and confidentiality are protected. - The model algorithms and outputs: The risk practitioner should validate that the model algorithms are appropriate, robust, and transparent for the access management process and the control objectives. The risk practitioner should also evaluate that the model outputs are accurate, reliable, and interpretable, and that they provide meaningful and actionable insights or recommendations for the access management process and the control objectives. - The model performance and monitoring: The risk practitioner should measure and monitor the model performance and effectiveness against the control objectives and the predefined metrics and indicators. The risk practitioner should also ensure that the model is updated and maintained regularly to reflect the changes in the access management process and the access rights, and that the model is audited and reviewed periodically to ensure its compliance and quality. By reviewing the design of the machine learning model against the control objectives, the risk practitioner can ensure that the model is fit for purpose and adds value to the access management process and the control objectives. The risk practitioner can also identify and mitigate any potential risks or issues that may arise from the use of the machine learning model as a control measure. References = Risk and Information Systems Control Study Manual, Chapter 3: Risk Response and Mitigation, Section 3.3: Control Design and Implementation, pp. 124-1271, Manage roles in your workspace - Azure Machine Learning2, Dataset Inference: Ownership Resolution in Machine Learning3

NEW QUESTION: 869
Which of the following is MOST helpful to ensure effective security controls for a cloud service provider?
A. A control self-assessment
B. A third-party security assessment report
C. Internal audit reports from the vendor
D. Service level agreement monitoring
Answer: (SHOW ANSWER)
A third-party security assessment report is the most helpful to ensure effective security controls for a cloud service provider, because it provides an independent and objective evaluation of the cloud provider's security posture, policies, and practices. A third-party security assessment report can help to verify and validate the cloud provider's compliance with the relevant standards, regulations, and best practices, such as ISO 27001, PCI DSS, NIST, or CSA. A third-party security assessment report can also help to identify and address any gaps, weaknesses, or vulnerabilities in the cloud provider's security controls, and to provide recommendations and guidance for improvement. A third-party security assessment report can also help to increase the trust and confidence of the cloud customers, and to facilitate the due diligence and risk management processes. The other options are less helpful to ensure effective security controls for a cloud service provider. A control self-assessment is a process that enables the cloud provider to assess its own security controls, using a predefined framework or questionnaire. However, a control self-assessment may not be as reliable or comprehensive as a third-party security assessment report, as it may be biased, incomplete, or inaccurate, and it may not cover all the aspects or dimensions of security. Internal audit reports from the vendor are documents that provide the results and findings of the internal audits conducted by the cloud provider's own auditors, to verify and validate the effectiveness and efficiency of the security

controls. However, internal audit reports from the vendor may not be as credible or trustworthy as a third-party security assessment report, as they may be influenced by the cloud provider's interests, objectives, or agenda, and they may not follow the same standards or criteria as the external auditors. Service level agreement monitoring is a process that measures and evaluates the performance and availability of the cloud services, based on the predefined metrics and targets agreed between the cloud provider and the cloud customer. However, service level agreement monitoring may not be sufficient or relevant to ensure effective security controls for a cloud service provider, as it may not address the security aspects or requirements of the cloud services, such as confidentiality, integrity, or accountability, and it may not reflect the actual security risks or incidents that may occur in the cloud environment. References = Cloud Security Controls: Key Elements and 4 Control Frameworks 1

NEW QUESTION: 870

Which of the following BEST enables the development of a successful IT strategy focused on business risk mitigation?

Freecram.net

A. Providing risk awareness training for business units
B. Obtaining input from business management
C. Understanding the business controls currently in place
D. Conducting a business impact analysis (BIA)
Answer: (SHOW ANSWER)
Obtaining input from business management is the best way to enable the development of a successful IT strategy focused on business risk mitigation, because it helps to align and integrate the IT objectives and activities with the business goals and priorities. An IT strategy is a plan that defines how IT supports and enables the organization's vision, mission, and strategy. A business risk mitigation is a process that aims to reduce or eliminate the risks that may affect the achievement of the business objectives or expectations. Obtaining input from business management is the best way to ensure that the IT strategy is relevant, realistic, and responsive to the business needs and challenges, and that the IT risks are identified, assessed, and managed in accordance with the business risk appetite and tolerance. Providing risk awareness training for business units, understanding the business controls currently in place, and conducting a business impact analysis (BIA) are all useful ways to support the development of an IT strategy focused on business risk mitigation, but they are not the best way, as they do not directly involve the input and feedback from business management. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.1.1, page 37

NEW QUESTION: 871
When developing IT risk scenarios, it is MOST important to consider:
A. The industry's threat profile.
B. Incidents occurring at similar organizations.
C. System performance thresholds.
D. Organizational objectives.
Answer: (SHOW ANSWER)

According to the CRISC Manual, developing IT risk scenarios must align with business objectives to ensure the scenarios are relevant and meaningful. A top-down approach driven by organizational objectives ensures scenarios are contextually appropriate and address what matters most to the enterprise. This ensures that risk management supports the enterprise's ability to achieve its mission and goals.
Reference:CRISC Manual - Domain 2: IT Risk Assessment, Slide 141-143

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 872
Which of the following BEST supports ethical IT risk management practices?
A. Robust organizational communication channels
B. Mapping of key risk indicators (KRIs) to corporate strategy
C. Capability maturity models integrated with risk management frameworks
D. Rigorously enforced operational service level agreements (SLAs)
Answer: (SHOW ANSWER)
Robust organizational communication channels are the best way to support ethical IT risk management practices, as they enable transparent and consistent sharing of risk information and decisions among all stakeholders. Ethical IT risk management requires that the risk management process and outcomes are aligned with the enterprise's values, objectives, and obligations, and that the risk management activities are conducted with integrity, accountability, and respect. Robust organizational communication channels facilitate these aspects by ensuring that the risk management roles and responsibilities are clearly defined and communicated, that the risk management policies and procedures are widely disseminated and understood, that the risk management performance and results are regularly reported and reviewed, and that the risk management feedback and improvement suggestions are solicited and addressed. Mapping of key risk indicators (KRIs) to corporate strategy, capability maturity models integrated with risk management frameworks, and rigorously enforced operational service level agreements (SLAs) are not directly related to ethical IT risk management practices, but rather to the effectiveness and efficiency of the risk management process. References = CRISC Certified in Risk and Information Systems Control - Question201; ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 201.

NEW QUESTION: 873
Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?
A. Risk exposure expressed in business terms
B. Recommendations for risk response options

C. Resource requirements for risk responses
D. List of business areas affected by the risk
Answer: (SHOW ANSWER)
Risk exposure is the potential loss or negative impact that may result from a risk. Expressing risk exposure in business terms means translating the technical or quantitative aspects of risk into meaningful and understandable information for the risk owner and other stakeholders. This can help the risk owner to make risk-aware decisions, as it can provide a clear and consistent basis for comparing and prioritizing risks, evaluating the cost-benefit of risk responses, and aligning the risk management strategy with the business objectives and value. The other options are not as helpful as risk exposure expressed in business terms, because they do not provide a comprehensive and relevant view of the risk, but rather focus on specific or partial aspects of the risk. References = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.3.1, page 45.

NEW QUESTION: 874
Which of the following is MOST important to ensure risk management practices are effective at all levels within the organization?
A. Communicating risk awareness materials regularly
B. Establishing key risk indicators (KRIs) to monitor risk management processes
C. Ensuring that business activities minimize inherent risk
D. Embedding risk management in business activities
Answer: (SHOW ANSWER)
Embedding Risk Management:
Integrated Approach: Embedding risk management in business activities ensures that risk considerations are part of everyday decision-making processes and operations.
Cultural Shift: Promotes a risk-aware culture where all employees understand their role in managing risk, leading to more proactive and effective risk management practices.
Comparison with Other Options:
Communicating Risk Awareness Materials: Important for education but less impactful than embedding risk management in daily activities.
Establishing KRIs: Useful for monitoring but does not ensure risk management practices are integrated into all business processes.
Minimizing Inherent Risk: This is an outcome of effective risk management rather than a method to ensure its effectiveness.
Best Practices:
Training and Awareness: Provide ongoing training to employees to embed risk management practices in their roles.
Policy and Procedures: Develop and enforce policies and procedures that integrate risk management into all business activities.
Leadership Support: Ensure strong support from leadership to promote and sustain a risk-aware culture.
References:

CRISC Review Manual: Emphasizes the importance of embedding risk management into business activities to ensure comprehensive and effective risk practices .
ISACA Guidelines: Support the integration of risk management into all levels of the organization to achieve effective risk management outcomes .

NEW QUESTION: 875
Which of the following should management consider when selecting a risk mitigation option?
A. Maturity of the enterprise architecture
B. Cost of control implementation
C. Reliability of key performance indicators (KPIs)
D. Reliability of key risk indicators (KPIs)
Answer: (SHOW ANSWER)
When selecting a risk mitigation option, management should consider the cost of control implementation, as well as the benefits and residual risks. The cost of control implementation includes the direct costs of acquiring, installing, and maintaining the control, as well as the indirect costs of potential side effects, such as reduced performance, increased complexity, or decreased user satisfaction. The cost of control implementation should be balanced with the expected reduction in risk exposure and the alignment with the enterprise's risk appetite and tolerance. The maturity of the enterprise architecture, the reliability of key performance indicators (KPIs), and the reliability of key risk indicators (KRIs) are relevant factors for risk identification and assessment, but not for risk response selection. References = Risk and Information Systems Control Study Manual, Chapter 4: Risk Response, page 149.

NEW QUESTION: 876
The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:
A. risk is treated appropriately
B. mitigating actions are prioritized
C. risk entries are regularly updated
D. risk exposure is minimized.
Answer: (SHOW ANSWER)
The primary reason to have risk owners assigned to entries in the risk register is to ensure that risk is treated appropriately, as risk owners are responsible for implementing the risk response strategies and monitoring the risk status and outcomes. Risk owners are also accountable for the risk and its impact on the enterprise's objectives and operations. Having risk owners assigned to entries in the risk register helps to clarify the roles and responsibilities, improve the communication and coordination, and enhance the effectiveness and efficiency of the risk management process. Mitigating actions are prioritized, risk entries are regularly updated, and risk exposure is minimized are not the primary reasons to have risk owners assigned to entries in the risk register, but rather the results or benefits of having risk owners assigned to entries in the risk register. References = CRISC by Isaca Actual Free Exam Q&As, question 206; CRISC: Certified in Risk & Information Systems Control Sample Questions, question 206.

NEW QUESTION: 877

The PRIMARY purpose of using control metrics is to evaluate the:
A. amount of risk reduced by compensating controls.
B. amount of risk present in the organization.
C. variance against objectives.
D. number of incidents.
Answer: (SHOW ANSWER)
The PRIMARY purpose of using control metrics is to evaluate the variance against objectives, because control metrics are measures that indicate the performance and effectiveness of the controls in achieving the desired outcomes and goals. Control metrics can help to identify and quantify the gaps or deviations between the actual and expected results of the controls, and to provide feedback and improvement for the control design and implementation. The other options are not the primary purpose, because:
Option A: Amount of risk reduced by compensating controls is a result of using control metrics, but not the primary purpose. Compensating controls are controls that provide an alternative or additional level of protection or assurance when the primary or preferred controls are not feasible or effective. Control metrics can help to measure and monitor the amount of risk reduced by compensating controls, but they are not the only or the most important measure of the control performance and effectiveness.
Option B: Amount of risk present in the organization is an input to using control metrics, but not the primary purpose. The amount of risk present in the organization is the level of exposure and uncertainty that the organization faces in pursuing its objectives and goals. Control metrics can help to assess and report the amount of risk present in the organization, but they are not the only or the most important measure of the risk profile and exposure.
Option D: Number of incidents is a source of using control metrics, but not the primary purpose. Incidents are events or occurrences that disrupt or threaten the normal operations or security of the organization. Control metrics can help to analyze and respond to the number of incidents, but they are not the only or the most important measure of the incident management and resolution. References = Risk and Information Systems Control Study Manual, 7th Edition, ISACA, 2020, p. 120.

NEW QUESTION: 878
A MAJOR advantage of using key risk indicators (KRIs) is that they:
A. Identify scenarios that exceed defined risk appetite.
B. Help with internal control assessments concerning risk appetite.
C. Assess risk scenarios that exceed defined thresholds.
D. Identify when risk exceeds defined thresholds.
Answer: (SHOW ANSWER)
KRIs provide measurable indicators that flag when risks exceed predefined thresholds, enabling swift and effective risk response. This supports theMonitoring and Reportingfunction in risk management, ensuring risks are managed proactively.

NEW QUESTION: 879
Which of the following BEST ensures that the data feeds used by an organization are complete and accurate?

A. Data is inspected and accepted by owners
B. Best-in-class data mining technology is used
C. Sources of data and attributes are known
D. The project is run by an experienced team
Answer: (SHOW ANSWER)
Whendata owners inspect and approveincoming data, it provides assurance of its completeness and accuracy, as they are accountable for the integrity of the data under their ownership.
Reference:CRISC Manual - Domain 2, Slide 132-135

NEW QUESTION: 880
Which of the following provides the MOST reliable evidence of a control's effectiveness?
A. A risk and control self-assessment
B. Senior management's attestation
C. A system-generated testing report
D. detailed process walk-through
Answer: (SHOW ANSWER)
The most reliable evidence of a control's effectiveness is a system-generated testing report. A system-generated testing report is a document that shows the results of automated tests performed by the system to verify that the control is functioning as intended and producing the expected outcomes. A system-generated testing report is reliable, because it is objective, consistent, accurate, and timely, and because it can provide a high level of assurance and confidence in the control's effectiveness. The other options are not as reliable as a system-generated testing report, although they may provide some evidence of the control's effectiveness. A risk and control self-assessment, senior management's attestation, and a detailed process walk-through are all examples of manual or subjective evidence, which may be prone to errors, biases, or inconsistencies, and which may provide a lower level of assurance and confidence in the control's effectiveness. References = Risk and Information Systems Control Study Manual, Chapter 3, Section 3.4.1, page 3-32.

NEW QUESTION: 881
Which of the following is the GREATEST concern associated with the lack of proper control monitoring?
A. There is potential for an increase in audit findings
B. Key performance indicators (KPIs) may not be reliable
C. The potential for risk realization is increased
D. Control inefficiencies may go undetected
Answer: (SHOW ANSWER)
Without monitoring, ineffective or failing controls may go unnoticed, leading to ahigher likelihood of risk eventsmaterializing, potentially with severe impact. This outweighs audit or KPI concerns.
Reference:CRISC Manual - Domain 4, Slide 386-390

NEW QUESTION: 882

Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

A. requirements of management.

B. specific risk analysis framework being used.

C. organizational risk tolerance

D. results of the risk assessment.

Answer: (SHOW ANSWER)

The results of risk analyses should be presented in quantitative or qualitative terms based primarily on the requirements of management, because they are the intended audience and users of the risk information, and they have the authority and responsibility to make risk-based decisions. The requirements of management may vary depending on the purpose, scope, and context of the risk analysis, and the level of detail, accuracy, and reliability that they need. Quantitative risk analysis uses numerical data and mathematical models to estimate the probability and impact of risks, and to express the risk exposure and value in monetary or other measurable units. Qualitative risk analysis uses descriptive data and subjective judgments to assess the likelihood and severity of risks, and to rank the risks according to their relative importance or priority. Both methods have their advantages and disadvantages, and they can be used separately or together, depending on the situation and the availability of data and resources. However, the primary factor that determines the choice of the method is the requirements of management, as they are the ones who will use the risk information to support their objectives, strategies, and actions. References = Risk IT Framework, ISACA, 2022, p. 141

NEW QUESTION: 883

While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

A. review and update the policies to align with industry standards.

B. determine that the policies should be updated annually.

C. report that the policies are adequate and do not need to be updated frequently.

D. review the policies against current needs to determine adequacy.

Answer: (SHOW ANSWER)

Information security policies are the foundation of an organization's security program, as they define the objectives, roles, responsibilities, and standards for protecting the information assets and systems. However, information security policies are not static, and they need to be reviewed and updated regularly to reflect the changes in the organization's environment, risk profile, and compliance requirements. Therefore, the best course of action when conducting an organization-wide risk assessment is to review the policies against current needs to determine adequacy. This means comparing the policies with the current threats, vulnerabilities, controls, and best practices, and identifying any gaps or weaknesses that need to be addressed.

The other options are not the best course of action, as they do not consider the current needs of the organization. Reviewing and updating the policies to align with industry standards may not be sufficient, as the organization may have specific or unique needs that are not covered by the standards. Determining that the policies should be updated annually may not be realistic, as the frequency of updates may depend on the

nature and complexity of the policies and the organization. Reporting that the policies are adequate and do not need to be updated frequently may not be accurate, as the policies may be outdated or ineffective, and may expose the organization to unnecessary risks. References = Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA, Does Your Organization Need a Security Risk Assessment? - ISACA, SP 800-39, Managing Information Security Risk: Organization, Mission ...

NEW QUESTION: 884
Which of the following is the PRIMARY objective of continuous monitoring?
A. Optimizing utilization of personnel
B. Aligning operations with policies and procedures
C. Detecting control errors in a timely manner
D. Minimizing the magnitude of loss from an event
Answer: (SHOW ANSWER)

NEW QUESTION: 885
Which of the following should a risk practitioner do NEXT after learning that Internet of Things (IoT) devices installed in the production environment lack appropriate security controls for sensitive data?
A. Assess the threat and associated impact.
B. Evaluate risk appetite and tolerance levels
C. Recommend device management controls
D. Enable role-based access control.
Answer: (SHOW ANSWER)
Assessing the threat and associated impact is the next thing that a risk practitioner should do after learning that Internet of Things (IoT) devices installed in the production environment lack appropriate security controls for sensitive data. This is because assessing the threat and associated impact can help determine the level and nature of the risk posed by the IoT devices, as well as the potential consequences and costs of a security breach or incident. Assessing the threat and associated impact can also provide the basis for further risk analysis and response steps, such as evaluating risk appetite and tolerance levels, recommending device management controls, or enabling role-based access control. According to the CRISC Review Manual 2022, assessing the threat and associated impact is one of the key steps in the IT risk assessment process1. According to the web search results, assessing the threat and associated impact is a common and recommended practice for addressing the security risks of IoT devices

NEW QUESTION: 886
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?
A. Relevance to the business process
B. Regulatory compliance requirements
C. Cost-benefit analysis
D. Comparison against best practice
Answer: (SHOW ANSWER)
The most important factor when deciding on a control to mitigate risk exposure is the cost-benefit analysis.

This is a process that compares the costs and benefits of implementing a control, and determines whether the control is worth the investment. A cost-benefit analysis helps to ensure that the control is efficient and effective in reducing the risk to an acceptable level, and that it does not introduce new risks or adversely affect other objectives. A cost-benefit analysis also helps to prioritize the controls based on their value and feasibility, and to allocate the resources accordingly. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.2.5, page 1861

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 887
Which of the following provides the MOST useful input to the development of realistic risk scenarios?
A. Balanced scorecard
B. Risk appetite
C. Risk map
D. Risk events
Answer: (SHOW ANSWER)
Risk events are specific occurrences or changes that have a potential impact on the achievement of objectives.
They can be positive or negative, and they can be internal or external to the organization. Risk events provide the basis for developing realistic risk scenarios, which are hypothetical situations that illustrate the possible consequences of a risk event. Risk scenarios help to understand and communicate the nature, sources, and causes of risk, as well as the potential impact and likelihood of risk occurrence. Risk scenarios can also be used to test the effectiveness of risk responses and controls.
The other options are not as useful as risk events for developing realistic risk scenarios. A balanced scorecard (A) is a strategic management tool that measures the performance of the organization against its objectives, vision, and strategy. It does not provide specific information about risk events or their consequences. A risk appetite (B) is the amount and type of risk that an organization is willing to accept in pursuit of its objectives.
It does not describe the risk events or their scenarios, but rather the level of risk tolerance and acceptance. A risk map is a graphical representation of the risk profile of the organization, showing the relationship between the likelihood and impact of different risks. It does not provide the details or context of the risk events or their scenarios, but rather the relative ranking and prioritization of risks.

NEW QUESTION: 888

A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

A. Document the finding in the risk register.

B. Invoke the incident response plan.

C. Re-evaluate key risk indicators.

D. Modify the design of the control.

Answer: (SHOW ANSWER)

The next step after determining that a key control does not meet design expectations is to document the finding in the risk register, because this helps to record and track the information about the identified risk, such as its description, likelihood, impact, response, and status. A key control is a control that addresses a significant risk or supports a critical business process or objective. A control design expectation is a criterion or requirement that defines how the control should operate or perform to achieve its objective. If a key control does not meet its design expectation, it means that there is a gap, weakness, or deficiency in the control that may compromise its effectiveness or efficiency, and increase the risk exposure or impact. By documenting the finding in the risk register, the risk practitioner can communicate and report the risk issue to the relevant stakeholders, such as the risk owner, the management, or the auditor, and initiate the appropriate risk response actions, such as modifying the design of the control, implementing a compensating control, or accepting the risk. The other options are not the best next steps after determining that a key control does not meet design expectations. Invoking the incident response plan is a reactive measure that is triggered when a risk event occurs or is imminent, and requires immediate action to contain, mitigate, or recover from the incident.

However, in this case, the risk event has not occurred yet, and there may be time to prevent or reduce it by improving the control design. Re-evaluating key risk indicators is a monitoring activity that measures and evaluates the level and impact of risks, and provides timely signals that something may be going wrong or needs urgent attention. However, in this case, the risk practitioner has already identified the risk issue, and needs to document and address it, rather than re-evaluate it. Modifying the design of the control is a possible risk response action that may be taken to improve the control and reduce the risk, but it is not the next step after determining that the key control does not meet design expectations. The next step is to document the finding in the risk register, and then decide on the best risk response action, which may or may not be modifying the design of the control, depending on the cost-benefit analysis, the risk assessment, and the risk response strategy. References = Risk IT Framework, ISACA, 2022, p. 13

NEW QUESTION: 889

Which of the following would BEST help an enterprise define and communicate its risk appetite?

A. Gap analysis

B. Risk assessment

C. Heat map

D. Risk register

Answer: (SHOW ANSWER)

The best way to help an enterprise define and communicate its risk appetite is to use a risk register, which is a document that records and summarizes the key information and data about the identified risks and the risk responses1. A risk register can help to:

* Define the risk appetite, which is the amount and type of risk that the enterprise is willing to accept or pursue in order to achieve its objectives2. The risk register can include the risk appetite statement, which is a clear and concise expression of the enterprise's risk preferences and boundaries3.
* Communicate the risk appetite, which is the process of sharing and informing the risk appetite to the relevant stakeholders, such as the board, the management, the employees, or the customers4. The risk register can be used as a communication tool, which can provide a consistent and transparent view of the enterprise's risk profile and performance5.

The other options are not the best ways to help an enterprise define and communicate its risk appetite, because:

* Gap analysis is a technique that compares the current state and the desired state of a process, system, or organization, and identifies the gaps or differences between them6. Gap analysis can help to assess the alignment or misalignment of the enterprise's risk appetite with its risk level, but it does not help to define or communicate the risk appetite itself.
* Risk assessment is a process that estimates the probability and impact of the risks, and prioritizes the risks based on their significance and urgency. Risk assessment can help to identify and analyze the risks that may affect the enterprise's objectives, but it does not help to define or communicate the risk appetite itself.
* Heat map is a graphical representation that uses colors to indicate the level or intensity of a variable, such as risk. Heat map can help to visualize and compare the risks based on their probability and impact, but it does not help to define or communicate the risk appetite itself.

References =

* Risk Register - CIO Wiki
* Risk Appetite - CIO Wiki
* Risk Appetite Statement - CIO Wiki
* Risk Communication - CIO Wiki
* Risk Reporting - CIO Wiki
* Gap Analysis - CIO Wiki
* [Risk Assessment - CIO Wiki]
* [Heat Map - CIO Wiki]
* [Risk and Information Systems Control documents and learning resources by ISACA]

NEW QUESTION: 890

Key risk indicators (KRIs) BEST support risk treatment when they:

A. Set performance expectations for controls.

B. Align with key business objectives.

C. Indicate that the risk is approaching predefined thresholds.

D. Articulate likelihood and impact in quantitative terms.

Answer: (SHOW ANSWER)

KRIs are most effective when they signal that a risk is nearing or exceeding predefined thresholds. This early warning enables organizations to take proactive measures to mitigate risks before they materialize into significant issues.
Reference:ISACA CRISC Review Manual, 7th Edition, Chapter 3: Risk Response and Reporting, Section: Key Risk Indicators.

NEW QUESTION: 891
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?
A. Key risk indicators (KRIs)
B. Key management indicators (KMIs)
C. Key performance indicators (KPIs)
D. Key control indicators (KCIs)
Answer: (SHOW ANSWER)
The best type of indicators to measure the effectiveness of an organization's firewall rule set are key control indicators (KCIs). A firewall is a device or software that filters the network traffic based on a set of rules or policies. A firewall rule set is the configuration of the firewall that defines the criteria for allowing or blocking the traffic. A key control indicator is a metric that measures the performance and effectiveness of a control in achieving its objectives and mitigating the risks. A key control indicator can help to evaluate the adequacy and efficiency of the firewall rule set, and to identify any gaps, weaknesses, or issues that need to be addressed. Key risk indicators (KRIs), key management indicators (KMIs), and key performance indicators (KPIs) are not as suitable as key control indicators, as they measure different aspects of the risk management process, such as the level and nature of the risk exposure, the alignment and integration of the risk management activities, and the achievement of the risk management goals and targets. References = CRISC Review Manual, 6th Edition, ISACA, 2015, page 220.

NEW QUESTION: 892
What is the PRIMARY purpose of a business impact analysis (BIA)?
A. To determine the likelihood and impact of threats to business operations
B. To identify important business processes in the organization
C. To estimate resource requirements for related business processes
D. To evaluate the priority of business operations in case of disruption
Answer: (SHOW ANSWER)
The primary purpose of a business impact analysis (BIA) is to evaluate the priority of business operations in case of disruption. A BIA is a process that identifies and analyzes the potential effects of various types of disruptions on the enterprise's critical business functions and processes. A BIA helps to determine the recovery objectives, such as the recovery time objective (RTO) and the recovery point objective (RPO), for each business operation, based on the impactof disruption on the enterprise's objectives, reputation, compliance, and stakeholders. A BIA also helps to identify the dependencies, resources, and interdependencies of the business operations, and to rank them according to their importance and urgency. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 2, Section

2.2.1, page 671

NEW QUESTION: 893
An organization is implementing data warehousing infrastructure. Senior management is concerned about safeguarding client data security in this new environment. Which of the following should the risk practitioner recommend be done NEXT?
A. Ensure an attribute-based access control model is implemented.
B. Ensure a role-based access control (RBAC) model is implemented.
C. Establish new controls addressing a consistently applied data access model.
D. Perform a gap analysis regarding the organization's client data access model.
Answer: (SHOW ANSWER)

NEW QUESTION: 894
Which of the following is MOST important to consider when selecting and designing key control indicators (KCIs)?
A. The KCI can establish a formal correlation with relevant KRIs
B. The KCI can demonstrate whether the control objective has been met
C. The KCI can be implemented within the allocated budget
D. The KCI can be measured using quantitative methods
Answer: (SHOW ANSWER)
The purpose of a Key Control Indicator (KCI) is to measure control effectiveness. Therefore, the most important design criterion is that it demonstrates whether the control objective is being achieved.
ISACA defines:
"KCIs are metrics that measure the effectiveness of controls in achieving their intended objectives."
Quantitative methods are desirable but secondary.
Hence, B is correct.
CRISC Reference: Domain 4 - Risk and Control Monitoring and Reporting, Topic: Control Performance Metrics.

NEW QUESTION: 895
Which of the following is MOST useful input when developing risk scenarios?
A. Common attacks in other industries.
B. Identification of risk events.
C. Impact on critical assets.
D. Probability of disruptive risk events.
Answer: (SHOW ANSWER)
Identifying specific risk events provides the foundational input for creating relevant and actionable risk scenarios. These scenarios form the basis of assessing potential impacts and determining effective controls. This is a key step in theRisk Identification and Assessmentprocess.

Valid CRISC Dumps shared by EduDump.com for Helping Passing CRISC Exam! EduDump.com now offer the **newest CRISC exam dumps**, the EduDump.com CRISC exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CRISC dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CRISC/premium/ (**1983** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)