ISACA.CISM.v2026-10-30.q493

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	493
Version:	v2026-10-30
# of views:	106
# of Questions views:	5360
https://www.freecram.net/torrent/ISACA.CISM.v2026-10-30.q493.html	

NEW QUESTION: 1
Which of the following would be MOST effective in reducing the impact of a distributed denial of service (DDoS) attack?
A. Impose state limits on servers.
B. Spread a site across multiple ISPs.
C. Block the attack at the source.
D. Harden network security.
Answer: B (LEAVE A REPLY)
The answer to the question is B. Spread a site across multiple ISPs. This is because spreading a site across multiple Internet service providers (ISPs) can help to reduce the impact of a distributed denial of service (DDoS) attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. Spreading a site across multiple ISPs can also help to distribute the traffic load and balance the performance of the site, and to mitigate the effects of regional or network-specific outages or disruptions. Spreading a site across multiple ISPs can be done by using various techniques, such as anycast routing, content delivery networks (CDNs), or cloud-based services12.
Spreading a site across multiple ISPs can help to reduce the impact of a DDoS attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; DDoS Attacks-A Cyberthreat and Possible Solutions2

NEW QUESTION: 2
Which of the following is the BEST way to determine the gap between the present and desired state of an information security program?
A. Perform a risk analysis for critical applications.
B. Determine whether critical success factors (CSFs) have been defined.

C. Conduct a capability maturity model evaluation.
D. Review and update current operational procedures.
Answer: (SHOW ANSWER)
A capability maturity model evaluation is the best way to determine the gap between the present and desired state of an information security program because it provides a systematic and structured approach to assess the current level of maturity of the information security processes and practices, and compare them with the desired or target level of maturity that is aligned with the business objectives and requirements. A capability maturity model evaluation can also help to identify the strengths and weaknesses of the information security program, prioritize the improvement areas, and develop a roadmap for achieving the desired state.
References = Information Security Architecture: Gap Assessment and Prioritization, CISM Review Manual
15th Edition

NEW QUESTION: 3
A business continuity plan (BCP) should contain:
A. data restoration procedures.
B. criteria for activation.
C. hardware and software inventories.
D. information about eradication activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
An information security manager of an e-commerce business is reviewing the results of a business continuity plan review. Which of the following findings should be the MOST immediate concern?
A. The business continuity plan has not been recently tested
B. The cost of a recent recovery test exceeded budget expectations
C. The annual business impact analysis has been delayed
D. The business continuity plan has not been recently audited
Answer: (SHOW ANSWER)
The correct answer is A because an untested business continuity plan creates immediate uncertainty about whether the organization can continue or recover critical operations during a disruption. For an e-commerce business, downtime can quickly affect revenue, customer trust, regulatory obligations, and service availability. Testing validates whether recovery procedures, people, technologies, communications, dependencies, and recovery objectives are realistic and achievable. A recovery test exceeding budget expectations is a concern, but it does not necessarily mean the organization cannot recover. A delayed business impact analysis is important because BIA supports continuity planning, but the immediate operational concern is that the plan has not been validated. A lack of recent audit may reduce assurance, but an audit is not a substitute for testing. In CISM, continuity and recovery capabilities must be tested to confirm

readiness and identify weaknesses before a real incident occurs. Therefore, the absence of recent BCP testing is the most immediate concern.
Reference: CISM Information Security Incident Management; business continuity, disaster recovery, plan testing, and operational resilience principles.

NEW QUESTION: 5
At what point should risk ownership be assigned?
A. When the risk treatment plan is executed
B. When asset ownership is assigned
C. When the risk is identified
D. When the related vulnerability is identified
Answer: (SHOW ANSWER)
Risk ownership should be assigned when the risk is identified (C). CISM emphasizes early assignment of ownership to ensure accountability for analysis, treatment decisions, and monitoring throughout the risk lifecycle. Waiting until treatment execution (A) delays accountability, while asset ownership (B) or vulnerability identification (D) alone does not ensure ownership of the broader business risk. Early ownership ensures risks are properly evaluated, escalated, and managed in line with risk appetite.
References: ISACA CISM Review Manual (Risk management-risk lifecycle and accountability); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 6
Which of the following should be done FIRST when a SIEM flags a potential event?
A. Validate the event is not a false positive.
B. Initiate the incident response plan.
C. Escalate the event to the business owner.
D. Implement compensating controls.
Answer: (SHOW ANSWER)
The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise.
A false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise. (From CISM Manual or related resources) References = CISM Review Manual 15th

Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 72, page 19

NEW QUESTION: 7
A business impact analysis (BIA) BEST enables an organization to establish:
A. restoration priorities.
B. annualized loss expectancy (ALE).
C. recovery methods.
D. total cost of ownership (TCO).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following is the BEST indication of effective information security governance?
A. Information security is considered the responsibility of the entire information security team.
B. Information security controls are assigned to risk owners.
C. Information security is integrated into corporate governance.
D. Information security governance is based on an external security framework.
Answer: (SHOW ANSWER)
Information security governance (ISG) is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk1. Effective ISG ensures that information security is integrated into corporate governance and is considered an essential component of enterprise governance2. Information security is not just the responsibility of the information security team, but of all stakeholders in the organization3. Information security controls are not assigned to risk owners, but to control owners who are accountable for implementing and maintaining the controls4. Information security governance is not based on an external security framework, but on the organization's own objectives, risk appetite, and compliance requirements. References = 1: CISM Review Manual (Digital Version), page 3 2:
CISM Review Manual (Digital Version), page 4 3: CISM Review Manual (Digital Version), page 5 4: CISM Review Manual (Digital Version), page 14 : CISM Review Manual (Digital Version), page 16

NEW QUESTION: 9
The PRIMARY consideration when responding to a ransomware attack should be to ensure:
A. backups are available.
B. the most recent patches have been applied.
C. the ransomware attack is contained
D. the business can operate
Answer: (SHOW ANSWER)

Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
* https://www.cisa.gov/stopransomware/ransomware-guide
* https://csrc.nist.gov/Projects/ransomware-protection-and-response
* https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

NEW QUESTION: 10

Which of the following business units should own the data that populates an identity management system?

Freecram.net

A. Information security
B. Information technology
C. Human resources (HR)
D. Legal
Answer: (SHOW ANSWER)

NEW QUESTION: 11

Which of the following activities is MOST appropriate to conduct during the eradication phase of a cyber incident response?
A. Estimate the amount of damage caused by the incident.
B. Restore affected systems for normal operations.
C. Mitigate exploited vulnerabilities to stop future incidents.
D. Isolate affected systems to prevent further damage
Answer: (SHOW ANSWER)

NEW QUESTION: 12

An organization's information security team presented the risk register at a recent information security steering committee meeting. Which of the following should be of MOST concern to the committee?
A. No owners were identified for some risks.
B. Business applications had the highest number of risks.
C. Risk mitigation action plans had no timelines.
D. Risk mitigation action plan milestones were delayed.
Answer: (SHOW ANSWER)

The most concerning issue for the information security steering committee should be that no owners were identified for some risks in the risk register. This means that there is no clear accountability and responsibility for managing and mitigating those risks, and that the risks may not be properly addressed or monitored. The risk owners are the persons who have the authority and ability to implement the risk treatment options and to accept the residual risk. The risk owners should be identified and assigned for each risk in the risk register, and they should report the status and progress of the risk management activities to the information security steering committee.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Management, Subsection: Risk Register, Page 104.

NEW QUESTION: 13
Which of the following is the PRIMARY benefit of an information security awareness training program?
A. Influencing human behavior
B. Evaluating organizational security culture
C. Defining risk accountability
D. Enforcing security policy
Answer: A (LEAVE A REPLY)
Influencing human behavior is the primary benefit of an information security awareness training program because it helps to reduce the human errors and vulnerabilities that can compromise the security of data and systems. An information security awareness training program is a process or a program that informs and empowers users to protect data and computing assets from security risks and cyberattacks. It includes educational offerings that cover regulatory requirements, compliance policies, and safe computing practices.
An information security awareness training program helps to influence human behavior by raising awareness of the security threats and challenges, enhancing knowledge and skills of the security best practices and controls, and fostering a positive security culture and attitude among the users. By influencing human behavior, an information security awareness training program can improve the security posture and performance of the organization, as well as prevent or mitigate the impact of security incidents. Therefore, influencing human behavior is the correct answer.
References:
* https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and-training/
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs
* https://threatcop.com/blog/benefits-and-purpose-of-security-awareness-training/.

NEW QUESTION: 14
Which of the following should an information security manager do NEXT after creating a roadmap to execute the strategy for an information security program?

A. Obtain consensus on the strategy from the executive board.
B. Review alignment with business goals.
C. Define organizational risk tolerance.
D. Develop a project plan to implement the strategy.
Answer: (SHOW ANSWER)
The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors. A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

NEW QUESTION: 15
The BEST way to report to the board on the effectiveness of the information security program is to present:
A. peer-group industry benchmarks.
B. a report of cost savings from process improvements.
C. a summary of the most recent audit findings.
D. a dashboard illustrating key performance metrics.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
An organization recently updated and published its information security policy and standards. What should the information security manager do NEXT?
A. Conduct a risk assessment.
B. Communicate the changes to stakeholders.
C. Update the organization's risk register.
D. Develop a policy exception process.
Answer: (SHOW ANSWER)
Communicating the changes to stakeholders is the next step after updating and publishing the information security policy and standards, as it ensures that the stakeholders are aware of the new or revised requirements, expectations and responsibilities, and can provide feedback or raise concerns if needed. Communication also helps to promote the acceptance and adoption of the policy and standards, and to reinforce the security culture and awareness within the organization.

(From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
Which of the following will have the MOST negative impact on the effectiveness of incident response processes?
A. Ambiguous severity criteria
B. High organizational risk tolerance
C. Decentralized incident monitoring
D. Manual incident reporting processes
Answer: (SHOW ANSWER)
The correct answer is A because ambiguous severity criteria can cause inconsistent classification, delayed escalation, inappropriate response actions, and poor prioritization during an incident. Incident response depends heavily on clear criteria for determining severity, impact, urgency, ownership, escalation paths, and communication requirements. If severity levels are unclear, responders may underestimate a serious incident or overreact to a minor event. This directly reduces the effectiveness of the response process. High organizational risk tolerance may influence response thresholds, but it does not necessarily make the process ineffective. Decentralized monitoring can create coordination challenges, but it can still be effective if roles and escalation processes are clear. Manual reporting may be slower than automated reporting, but it can still work if the process is well-defined. CISM emphasizes that incident response processes require classification, prioritization, escalation, and communication procedures. Clear severity criteria are foundational to effective incident management because they guide timely and appropriate response decisions.
Reference: CISM Information Security Incident Management; incident classification, severity criteria, escalation, and response process principles.

NEW QUESTION: 18
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?
A. Regulations and standards
B. People and culture

C. Executive and board directives
D. Processes and technology
Answer: (SHOW ANSWER)
A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have a higher chance of achieving its objectives and improving the overall security posture of the organization.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

NEW QUESTION: 19
Who is BEST suited to determine how the information in a database should be classified?
A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner
Answer: (SHOW ANSWER)
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements.
Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331

NEW QUESTION: 20

Which of the following is the BEST control to protect customer personal information that is stored in the cloud?

Freecram.net

A. Timely deletion of digital records
B. Appropriate data anonymization
C. Strong encryption methods
D. Strong physical access controls
Answer: (SHOW ANSWER)
Strong encryption methods are the BEST control to protect customer personal information that is stored in the cloud, because they help to prevent unauthorized access, disclosure, modification, or deletion of the data by encrypting it at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data. Encryption can help to protect the confidentiality, integrity, and availability of the data, as well as to comply with legal and regulatory requirements.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Encryption is the process of transforming data into an unreadable format using a secret key or algorithm." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Encryption can help to protect the confidentiality, integrity, and availability of data, as well as to comply with legal and regulatory requirements for data protection." Saas Data Security: Protecting Your Customers' Information In The Cloud - Fresent's Blog: "Encryption and Data Protection: One of the most effective ways to protect sensitive data in the cloud is to encrypt it both at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data."

NEW QUESTION: 21
Which of the following BEST indicates the effectiveness of the vendor risk management process?
A. Increase in the percentage of vendors certified to a globally recognized security standard
B. Increase in the percentage of vendors with a completed due diligence review
C. Increase in the percentage of vendors conducting mandatory security training
D. Increase in the percentage of vendors that have reported security breaches
Answer: (SHOW ANSWER)
This answer best indicates the effectiveness of the vendor risk management process because it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices.
A globally recognized security standard, such as ISO 27001, NIST CSF, or COBIT, provides a comprehensive and objective framework for assessing and improving the security posture and performance of vendors.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security requirements and expectations for third-party products

and services are defined, communicated, and enforced" and that "the information security manager should verify that the third parties have implemented adequate security controls and practices, and that they comply with applicable standards and regulations" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Increase in the percentage of vendors certified to a globally recognized security standard is the correct answer because it best indicates the effectiveness of the vendor risk management process, as it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices" (p. 63). Additionally, the article Vendor Risk Management Demystified from the ISACA Journal 2015 states that "a globally recognized security standard provides a common language and framework for evaluating and improving the security posture and performance of vendors" and that "a vendor certification to a globally recognized security standard can help to reduce the risk of security breaches, increase the trust and confidence of customers and stakeholders, and enhance the reputation and competitiveness of the vendor" (p. 3

NEW QUESTION: 22
Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?
A. Conduct a cost-benefit analysis.
B. Consult corporate legal counsel
C. Update the information security policy.
D. Perform a gap analysis.
Answer: (SHOW ANSWER)
When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 23
Security administration efforts will be greatly reduced following the deployment of which of the following techniques?
A. Discretionary access control
B. Role-based access control
C. Access control lists
D. Distributed access control

Answer: (SHOW ANSWER)
Role-based access control (RBAC) is a policy-neutral access control mechanism that assigns access privileges to defined roles in the organization and then makes each user a member of the appropriate roles.
RBAC reduces security administration efforts by simplifying the management of access rights across different users and resources. RBAC also enables consistent and efficient enforcement of the principle of least privilege, which grants users only the minimum rights required to perform their assigned tasks. RBAC can also facilitate the implementation of separation of duties, which prevents users from having conflicting or incompatible responsibilities. RBAC is among the most widely used methods in the information security tool kit1. References = CIS Control 6: Access Control Management - Netwrix, CISSP certification: RBAC (Role based access control), What is RBAC? (Role Based Access Control) - IONOS

NEW QUESTION: 24
During which phase of a security event should an incident response team be INITIALLY engaged?
A. Preparation
B. Eradication
C. Identification
D. Recovery
Answer: (SHOW ANSWER)
The correct answer is C because the incident response team should be initially engaged when a security event is identified as potentially requiring investigation, validation, classification, or escalation. The identification phase involves detecting, reporting, analyzing, and determining whether an event is actually an incident. Early engagement of the incident response team helps ensure the event is validated, categorized, prioritized, and handled according to the incident response plan. Preparation is an important phase in the incident management life cycle, but it occurs before a specific security event and involves planning, training, tools, and readiness. Eradication occurs after the incident is confirmed and containment activities have begun. Recovery occurs after the threat has been removed and services are being restored. CISM emphasizes timely detection, identification, classification, escalation, and response to reduce business impact. Since the question asks when the team should be engaged during a security event, the best answer is the identification phase.
Reference: CISM Information Security Incident Management; incident identification, validation, escalation, classification, and response life cycle principles.

NEW QUESTION: 25
Which of the following is the FIRST step when conducting a post-incident review?
A. Identify mitigating controls.
B. Assess the costs of the incident.
C. Perform root cause analysis.

D. Assign responsibility for corrective actions.

Answer: (SHOW ANSWER)

A post-incident review is a process of analyzing an incident and its impact, identifying the root causes, and recommending corrective actions to prevent recurrence. The first step of a post-incident review is to perform root cause analysis, which is the process of identifying the underlying factors that contributed to the occurrence and severity of the incident. Root cause analysis helps to determine the most effective and efficient solutions to address the problem and avoid future incidents. References = CISM Review Manual,
16th Edition, Chapter 5, Section 5.5.2.11

NEW QUESTION: 26

A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:

A. developing a security program that meets global and regional requirements.

B. ensuring effective communication with local regulatory bodies.

C. using industry best practice to meet local legal regulatory requirements.

D. monitoring compliance with defined security policies and standards.

Answer: (SHOW ANSWER)

= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. References = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.

In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

NEW QUESTION: 27

Which of the following is a PRIMARY function of an incident response team?
A. To provide a business impact analysis
B. To provide a risk assessment for zero-day vulnerabilities
C. To provide effective incident mitigation
D. To provide a single point of contact for critical incidents
Answer: C (LEAVE A REPLY)
The correct answer is C because the primary purpose of an incident response team is to respond to security incidents and reduce their impact through effective mitigation. Incident response teams investigate incidents, classify severity, contain threats, coordinate response actions, support eradication, assist recovery, and help prevent recurrence through lessons learned. A business impact analysis is generally part of business continuity planning, not the primary responsibility of the incident response team. A risk assessment for zero-day vulnerabilities is part of risk management and vulnerability management, not the core incident response function. Acting as a single point of contact for critical incidents may be one responsibility of the team or incident coordinator, but it is not the primary function. CISM incident management emphasizes timely detection, response, containment, communication, recovery, and post-incident improvement. The team exists mainly to reduce business harm from incidents. Therefore, providing effective incident mitigation is the best answer.
Reference: CISM Information Security Incident Management; incident response team responsibilities, mitigation, containment, and impact reduction principles.

NEW QUESTION: 28
Which of the following is MOST important when responding to a major security incident?
A. Contacting forensic investigators
B. Following the escalation process
C. Notifying law enforcement
D. Identifying the indicators of compromise
Answer: (SHOW ANSWER)
Following the escalation process ensures that the incident is managed in accordance with established protocols, involving the right stakeholders and prioritizing the incident appropriately.
"Following the escalation process is critical to ensure that incidents are handled appropriately and that the right personnel are engaged at the right time."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Escalation Procedures* ISACA practice questions highlight that proper escalation is vital to ensure incidents are managed effectively and consistently.

NEW QUESTION: 29
Which of the following is the PRIMARY benefit of training service desk staff to recognize incidents?
A. Incident response plan can be activated in a timely manner.
B. Incident metrics can be communicated.

C. Risk response options can be identified quickly.
D. Incident classification times can be improved.
Answer: (SHOW ANSWER)
The service desk is often the first point of contact for users. If trained properly, they can quickly recognize signs of an incident and escalate it, triggering the incident response process promptly. This early detection and escalation are essential for minimizing damage and response time.
"Training frontline support staff ensures timely detection and escalation of incidents, which is critical for effective containment."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Roles and Responsibilities*

NEW QUESTION: 30
An organization wants to integrate information security into its HR management processes. Which of the following should be the FIRST step?
Freecram.net
A. Benchmark the processes with best practice to identify gaps.
B. Calculate the return on investment (ROI).
C. Provide security awareness training to HR.
D. Assess the business objectives of the processes.
Answer: (SHOW ANSWER)
The first step when integrating information security into HR management processes is to assess the business objectives of the processes, which means understanding the purpose, scope, and expected outcomes of the HR functions and activities, and how they relate to the organization's strategy and goals. The assessment will help to identify the information security requirements, risks, and controls that are relevant and applicable to the HR processes, and to align the information security objectives with the business objectives.
References = CISM Review Manual 15th Edition, CISM: Overview of domains [updated 2022]

NEW QUESTION: 31
When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to:
A. the incident response process to stakeholders
B. adequately staff and train incident response teams.
C. develop effective escalation and response procedures.
D. make tabletop testing more effective.
Answer: (SHOW ANSWER)
The primary benefit of establishing a clear definition of a security incident is that it helps to develop effective escalation and response procedures. A security incident is an event or an attempt that disrupts or threatens the normal operations, security, or privacy of an organization's information or systems1. A clear definition of a security in-cident helps to:
*Distinguish between normal and abnormal events, and between security-relevant and non-security-relevant events

*Determine the severity and impact of an incident, and the appropriate level of response
*Assign roles and responsibilities for incident detection, reporting, analysis, containment, eradication, recovery, and post-incident activities
*Establish criteria and thresholds for escalating incidents to higher authorities or external parties
*Define the communication channels and protocols for incident notification and coordina-tion
*Document the incident response process and procedures in a formal plan According to NIST, a clear definition of a security incident is one of the key compo-nents of an effective incident response capability2. The other options are not the prima-ry benefits of establishing a clear definition of a security incident. Communicating the incident response process to stakeholders is important, but it is not the main purpose of defining a security incident. Adequately staffing and training incident response teams is essential, but it depends on other factors besides defining a security inci-dent. Making tabletop testing more effective is a possible outcome, but not a direct benefit of defining a security incident. References: 2: NIST SP
800-61 Rev. 2 Computer Security Incident Handling Guide 1: NIST Glossary - Security Incident : What is a securi-ty incident? - TechTarget : 10 types of security incidents and how to handle them - TechTarget : 45 CFR § 164.304 - Definitions - Electronic Code of Federal Regulations

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
When determining an acceptable risk level which of the following is the MOST important consideration?
A. Threat profiles
B. System criticalities
C. Vulnerability scores
D. Risk matrices
Answer: (SHOW ANSWER)
The effectiveness of an incident response team will be greatest when the incident response process is updated based on lessons learned. This ensures that the team can continuously improve its performance and capabilities, and address any gaps or weaknesses identified during previous incidents. Updating the incident response process based on lessons learned also helps to align the process with the changing business and security environment, and to incorporate best practices and standards. Meeting on a regular basis to review log files, having trained security personnel as team members, and using a security information and event monitoring (SIEM)

system are all important factors for an incident response team, but they are not sufficient to ensure the effectiveness of the team. Reviewing log files may help to detect and analyze incidents, but it does not guarantee that the team can respond appropriately and efficiently. Having trained security personnel may enhance the skills and knowledge of the team, but it does not ensure that the team can work collaboratively and communicate effectively. Using a SIEM system may facilitate the identification and prioritization of incidents, but it does not ensure that the team can follow the established procedures and protocols. References = CISM Review Manual, 16th Edition, page 1361; CISM Review Questions, Answers
& Explanations Manual, 10th Edition, page 1492

NEW QUESTION: 33
During the selection of a Software as a Service (SaaS) vendor for a business process, the vendor provides evidence of a globally accepted information security certification. Which of the following is the MOST important consideration?
A. The certification includes industry-recognized security controls.
B. The certification was issued within the last five years.
C. The certification is issued for the specific scope.
D. The certification is easily verified.
Answer: (SHOW ANSWER)
The most important consideration when selecting a SaaS vendor for a business process is whether the vendor' s information security certification is issued for the specific scope of the service that the organization needs. A certification that covers the entire vendor organization or a different service may not be relevant or sufficient for the organization's security requirements. The certification should also include industry-recognized security controls, be issued within a reasonable time frame, and be easily verified, but these are not as critical as the scope. References = CISM Review Manual, 16th Edition, page 1841; 5 Top SaaS Security Certifications for SaaS Providers

NEW QUESTION: 34
In the context of developing an information security strategy, which of the following provides the MOST useful input to determine the or
A. Security budget
B. Risk register
C. Risk score
D. Laws and regulations
Answer: (SHOW ANSWER)
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security

needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with- business-goals-and-objectives

NEW QUESTION: 35
An organization is MOST likely to accept the risk of noncompliance with a new regulatory requirement when:
A. employees are resistant to the controls required by the new regulation.
B. the regulatory requirement conflicts with business requirements.
C. the risk of noncompliance exceeds the organization's risk appetite.
D. the cost of complying with the regulation exceeds the potential penalties.
Answer: (SHOW ANSWER)
An organization is most likely to accept the risk of noncompliance with a new regulatory requirement when the cost of complying with the regulation exceeds the potential penalties. In such cases, from a cost-benefit perspective, the organization might find it more economical to absorb potential fines or penalties rather than implementing costly controls or processes to comply with the regulation.
"Risk acceptance occurs when the cost of mitigating or transferring the risk exceeds the benefit of the mitigation. This also applies to regulatory noncompliance if the penalties are less than the costs of compliance."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* ISACA's practice questions highlight that risk acceptance is a legitimate treatment when costs outweigh potential penalties or impact.

NEW QUESTION: 36
Which of the following BEST enables an organization to enhance its incident response plan processes and procedures?
A. Security risk assessments
B. Lessons learned analysis
C. Information security audits
D. Key performance indicators (KPIs)
Answer: (SHOW ANSWER)
Lessons learned analysis is the best way to enable an organization to enhance its incident response plan processes and procedures because it helps to identify the strengths and

weaknesses of the current plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Security risk assessments are not directly related to enhancing the incident response plan, but rather to identifying and evaluating the security risks and controls of the organization. Information security audits are not directly related to enhancing the incident response plan, but rather to verifying and validating the compliance and effectiveness of the security policies and standards of the organization. Key performance indicators (KPIs) are not directly related to enhancing the incident response plan, but rather to measuring and reporting the performance and progress of the security objectives and initiatives of the organization.
References: https://www.isaca.org/resources/isaca-journal/issues
/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2017
/volume-1/security-risk-assessment-for-a-cloud-based-enterprise-resource-planning-system https://www.isaca.
org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security- using-iso-27004 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the- effectiveness-of-your-information-security-management-system

NEW QUESTION: 37
Which of the following is the PRIMARY impact of organizational culture on the effectiveness of an information security program?
A. The culture shapes behaviors toward information security.
B. The culture defines responsibilities necessary for program implementation.
C. The culture helps determine budget for information security controls.
D. The culture has minimal impact as long as information security controls are adhered to.
Answer: (SHOW ANSWER)
A culture that supports security encourages behaviors that protect information assets.
"Organizational culture has a significant impact on how employees approach security, influencing their behavior and adherence to policies."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture*

NEW QUESTION: 38
Detailed business continuity plans (BCPs) should be PRIMARILY based on:
A. capabilities of available local vendors.
B. strategies that cover all applications.
C. cost and resources needed to execute.
D. strategies validated by senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following processes determines whether an event gets classified as an incident?
A. Threat intelligence reviews
B. End-user reporting
C. Triage
D. Business impact analysis
Answer: (SHOW ANSWER)
The correct answer is C because triage is the process used to evaluate a detected or reported event and determine whether it should be classified as an incident. During triage, the security team reviews available evidence, validates alerts, determines severity, assesses potential impact, identifies affected assets, and decides whether escalation is required. Threat intelligence reviews help identify emerging threats or indicators of compromise, but they do not determine whether a specific event is an incident. End-user reporting is an important source of event detection, but reports must still be analyzed and validated. A business impact analysis is used for continuity planning and determining the impact of disruptions, not for classifying individual security events.
In CISM incident management, events must be identified, analyzed, categorized, prioritized, and escalated through a structured process. Triage is the key step that separates normal events, false positives, security events, and confirmed incidents.
Reference: CISM Information Security Incident Management; event triage, incident identification, classification, prioritization, and escalation principles.

NEW QUESTION: 40
When investigating an information security incident, details of the incident should be shared:
A. widely to demonstrate positive intent.
B. only with management.
C. only as needed,
D. only with internal audit.
Answer: (SHOW ANSWER)
When investigating an information security incident, details of the incident should be shared only as needed, according to the principle of least privilege and the need-to-know basis. This means that only the authorized and relevant parties who have a legitimate purpose and role in the incident response process should have access to the incident information, and only to the extent that is necessary for them to perform their duties.
Sharing incident details only as needed helps to protect the confidentiality, integrity, and availability of the incident information, as well as the privacy and reputation of the affected individuals and the organization.
Sharing incident details only as needed also helps to prevent unauthorized disclosure, modification, deletion, or misuse of the incident information, which could compromise the investigation, evidence, remediation, or legal actions.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, page 2311; CISM Review Questions, Answers & Explanations Manual,
10th Edition, Question 49, page 462.

NEW QUESTION: 41
Which of the following is the MOST appropriate response to a highly sophisticated new ransomware threat?
A. Implement immutable backups
B. Purchase cybersecurity insurance
C. Deploy a new anti-malware solution
D. Upgrade firewall protection
Answer: (SHOW ANSWER)
The correct answer is A because immutable backups provide strong resilience against ransomware by preventing backup data from being altered, encrypted, or deleted during an attack. Sophisticated ransomware often attempts to compromise backups before encrypting production systems, making ordinary backups insufficient if they can be modified by attackers. Immutable backups preserve clean recovery points and support restoration after containment and eradication. Cybersecurity insurance may transfer some financial risk, but it does not prevent data loss or restore operations by itself. A new anti-malware solution may help detect known ransomware, but sophisticated new threats may evade signature-based or behavioral detection. Upgrading firewall protection may reduce some network exposure, but ransomware commonly enters through phishing, compromised credentials, vulnerable services, or supply chain channels. CISM incident management and resilience principles emphasize maintaining recovery capability for disruptive attacks.
Immutable backups are therefore the most appropriate response because they directly support recovery from ransomware impact.
Reference: CISM Information Security Incident Management; ransomware resilience, immutable backups, disaster recovery, and recovery capability principles.

NEW QUESTION: 42
An information security manager has been asked to provide contract guidance from a security perspective for outsourcing the organization's payroll processing. Which of the following is MOST important to address?
A. Vendor compliance with the most stringent data security regulations
B. Vendor compliance with recognized industry security standards
C. Vendor compliance with the organization's information security policies
D. Vendor compliance with organizational service level agreement requirements
Answer: (SHOW ANSWER)
The correct answer is C because an outsourced payroll provider will process sensitive employee information, and the contract must require the vendor to comply with the organization's

information security policies or equivalent security requirements. Payroll data may include personally identifiable information, salary details, tax information, bank account data, and employment records. The organization remains accountable for protecting this information even when processing is outsourced. Recognized industry standards are useful, but they may not fully reflect the organization's specific policy requirements, risk appetite, privacy obligations, access rules, incident notification needs, or data handling expectations. The most stringent regulations may not always be applicable, and contract requirements should be based on relevant legal, regulatory, and organizational obligations. Service level agreements are important for performance and availability, but they do not fully address security governance. In CISM third-party risk management, contracts should include security requirements aligned with organizational policies, compliance obligations, audit rights, confidentiality, incident reporting, and control expectations. Therefore, vendor compliance with the organization's information security policies is most important.
Reference: CISM Information Risk Management; third-party risk, outsourcing, payroll data protection, contractual security requirements, and vendor compliance principles.

NEW QUESTION: 43
Which of the following is MOST important to verify during a test of an organization's incident response process?
A. Whether users know which numbers to call in the call tree
B. Whether incident response team members know their responsibilities
C. Whether incident response team members are cross-trained
D. Whether senior management endorses the incident response process
Answer: (SHOW ANSWER)
The most important item to verify during an incident response test is whether incident response team members know their responsibilities. CISM incident management emphasizes that effective response depends on clearly defined and understood roles, responsibilities, escalation paths, and decision authority. During a real incident, confusion about who must contain, investigate, communicate, approve, or recover systems can cause delays and increase business impact. Users knowing call-tree numbers is useful, but the response team's execution responsibilities are more central to incident handling. Cross-training is valuable for resilience, but it is secondary to each team member understanding their assigned role. Senior management endorsement is important for governance and support, but it is not what an operational test primarily validates. Incident response testing should determine whether the process works in practice, including coordination, communication, containment, escalation, and recovery. Therefore, verifying that response team members understand their responsibilities is the most important objective of the test.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident response testing, roles, and responsibilities ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 44
Which of the following is the PRIMARY reason to regularly update business continuity and disaster recovery documents?
A. To enforce security policy requirements
B. To maintain business asset inventories
C. To ensure audit and compliance requirements are met
D. To ensure the availability of business operations
Answer: (SHOW ANSWER)
The primary reason to regularly update business continuity and disaster recovery documents is to ensure that the plans and procedures are aligned with the current business needs and objectives, and that they can effectively support the availability of business operations in the event of a disaster. Updating the documents also helps to enforce security policy requirements, maintain business asset inventories, and ensure audit and compliance requirements are met, but these are secondary benefits.
References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Business Continuity Planning, Subsection: Business Continuity Plan Maintenance, Page
378.

NEW QUESTION: 45
Which of the following is the BEST justification for making a revision to a password policy?
A. Vendor recommendation
B. Audit recommendation
C. A risk assessment
D. Industry best practice
Answer: (SHOW ANSWER)
The best justification for making a revision to a password policy is a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a risk assessment, the organization can determine the appropriate level of security controls and measures to protect its information assets and systems, including password policies. A risk assessment can also help identify any gaps or weaknesses in the existing password policy, and provide recommendations for improvement based on the organization's risk appetite and tolerance. The other options are not the best justification for making a revision to a password policy, although they may be some inputs or outputs of the risk assessment process. A vendor recommendation is an external source of advice or guidance that may or may not be relevant or applicable to the organization's specific context and needs. A vendor recommendation should not be followed blindly without conducting a risk assessment to evaluate its suitability and effectiveness. An audit recommendation is an internal source of feedback or suggestion that may or may not be accurate or complete.

An audit recommendation should not be implemented without conducting a risk assessment to verify its validity and feasibility. An industry best practice is a general standard or guideline that may or may not reflect the organization's unique characteristics and requirements. An industry best practice should not be adopted without conducting a risk assessment to customize it according to the organization's goals and priorities

NEW QUESTION: 46
A business impact analysis (BIA) should be periodically executed PRIMARILY to:
A. validate vulnerabilities on environmental changes.
B. analyze the importance of assets.
C. check compliance with regulations.
D. verify the effectiveness of controls.
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12.
According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations ©, as these are not the primary purposes of a BIA.
References: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 47
Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?
A. Implement mitigating actions immediately.
B. Invoke the incident response plan.

C. Inform senior management of the breach.
D. Validate the breach.
Answer: D (LEAVE A REPLY)
The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions.
Invoking the incident response plan or informing management comes after the breach is validated.
Reference:ISACA CISM Review Manual, 16th Edition, Page 280, "Incident Detection and Validation".

NEW QUESTION: 48
Which of the following roles is PRIMARILY responsible for developing an information classification framework based on business needs?
A. Information security manager
B. Information security steering committee
C. Information owner
D. Senior management
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, Information owners are responsible for developing an information classification framework based on business needs1. They are also responsible for defining and maintaining the classification scheme, policies, and procedures for their information assets1.
The CISM Review Manual (Digital Version) also states that information owners should collaborate with other stakeholders, such as information security managers, information security steering committees, senior management, and legal counsel, to ensure that the classification framework is aligned with the organization's objectives and complies with applicable laws and regulations1.
The CISM Exam Content Outline also covers the topic of information classification frameworks in Domain 3
- Information Security Program Development and Management (27% exam weight)2. The subtopics include:
* 3.2.1 Information Classification Frameworks
* 3.2.2 Information Classification Policies
* 3.2.3 Information Classification Procedures
* 3.2.4 Information Classification Training
I hope this answer helps you prepare for your CISM exam. Good luck! #

NEW QUESTION: 49
Identifying which of the following BEST enables a cyberattack to be contained?
A. The IP address of the computer that launched the attack

B. The segment targeted by the attack
C. The threat actor that initiated the attack
D. The vulnerability exploited by the attack
Answer: (SHOW ANSWER)

NEW QUESTION: 50
After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?
Freecram.net
A. The service level agreement (SLA) was not met.
B. The recovery time objective (RTO) was not met.
C. The root cause was not identified.
D. Notification to stakeholders was delayed.
Answer: (SHOW ANSWER)
= After a ransomware incident, the most important concern for the information security manager is to identify the root cause of the incident and prevent it from happening again. The root cause analysis (RCA) is a systematic process of finding and eliminating the underlying factors that led to the incident, such as vulnerabilities, misconfigurations, human errors, or malicious actions. Without performing a RCA, the organization may not be able to address the root cause and may face the same or similar incidents in the future, which could result in more damage, costs, and reputational loss. Therefore, the information security manager should prioritize the RCA over other concerns, such as meeting the SLA, RTO, or notification requirements, which are important but secondary to the RCA.
References = CISM Review Manual 15th Edition, page 254-2551; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 4202

NEW QUESTION: 51
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?
A. The benefit is greater than the potential risk.
B. USB storage devices are enabled based on user roles.
C. Users accept the risk of noncompliance.
D. Access is restricted to read-only.
Answer: (SHOW ANSWER)
The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security pol-icy should also be aligned with the organization's business objectives

and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2.
The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as:
*Enhancing data mobility and accessibility
*Improving data backup and recovery
*Supporting data sharing and collaboration
*Enabling data encryption and authentication
However, USB storage devices also pose significant security risks for users and organi-zations, such as:
*Introducing malware or viruses to laptops and desktops
*Exposing sensitive data to unauthorized access or disclosure
*Losing or stealing data due to device loss or theft
*Violating security policies or regulations
Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4.
Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5.
References: 1:
Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

NEW QUESTION: 52
Which of the following is MOST important to ensure incident management readiness?
A. The plan is compliant with industry standards.
B. The plan is regularly tested.
C. The plan is updated annually.
D. The plan is concise and includes a checklist.
Answer: (SHOW ANSWER)
Regular testing ensures that the incident management plan is practical and effective in real-world scenarios.
"Regular testing of the incident response plan is essential to verify that it can be executed effectively and that staff understand their roles."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Testing and Evaluation*

NEW QUESTION: 53
Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?
A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards
Answer: (SHOW ANSWER)
= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION: 54
An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?
A. Initiate incident response.
B. Disable remote
C. Initiate a device reset.
D. Conduct a risk assessment.
Answer: (SHOW ANSWER)

Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage.
According to ISACA, incident management is one of the key processes for information security governance.
Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan. References: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

NEW QUESTION: 55
Which of the following is the MOST important benefit of using a cloud access security broker when migrating to a cloud environment?
A. Enhanced data governance
B. Increased third-party assurance
C.)Improved incident management
D. Reduced total cost of ownership (TCO)
Answer: (SHOW ANSWER)
According to the web search results, a cloud access security broker (CASB) is a software solution that stands between the cloud service provider and the cloud service user to enforce security controls. One of the most important benefits of using a CASB when migrating to a cloud environment is enhanced data governance, as it helps to protect sensitive information from unauthorized access, sharing, or loss. A CASB can also provide data classification, encryption, data loss prevention (DLP), and other features that enable organizations to manage and secure their data in the cloud.
References = What Is a Cloud Access Security Broker (CASB)?, A beginner's guide to cloud access security brokers

NEW QUESTION: 56
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. Risk mitigation strategy
B. Security 'strategy
C. IT strategy
D. Recovery strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 57

Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.

B. Internal compliance requirements are being met.

C. Risk management objectives are being met.

D. Business needs are being met.

Answer: (SHOW ANSWER)

The primary purpose of business continuity and disaster recovery plans is to ensure that the organization can resume its critical business functions within the stated recovery time objectives (RTOs) after a disruptive event. RTOs are based on the business needs and the impact analysis of each function or process. Therefore, meeting the business needs is the best indicator that the plans are effective. Regulatory requirements, internal compliance requirements, and risk management objectives are important factors that influence the development and testing of the plans, but they are not the ultimate measure of their effectiveness. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3071; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Imperva, Business Continuity & Disaster Recovery Planning (BCP & DRP)3

NEW QUESTION: 58

What will BEST facilitate the success of new security initiatives?

A. Monitor post-implementation security metrics

B. Establish an IT security steering committee

C. Update security policies on a regular basis

D. Include business in security decision-making

Answer: (SHOW ANSWER)

The correct answer is D because new security initiatives are most successful when the business is included in security decision-making. Business involvement helps ensure that initiatives address real business risks, align with strategic objectives, receive appropriate support, and are practical for operational adoption. Security initiatives that are developed without business input may face resistance, poor funding, limited adoption, or misalignment with priorities. Monitoring post-implementation metrics is important, but it occurs after implementation and does not by itself ensure success. Establishing an IT security steering committee may support governance, but the wording is narrower than business-wide involvement and may remain too IT- focused. Updating security policies regularly is good practice, but policies alone do not guarantee initiative success. CISM governance emphasizes business alignment, stakeholder engagement, accountability, and value delivery. Including business stakeholders in security decisions ensures shared ownership and improves the likelihood that security initiatives will be accepted and effective.
Reference: CISM Information Security Governance; business involvement, stakeholder engagement, security initiative success, and strategic alignment principles.

NEW QUESTION: 59
Which of the following BEST informs the design of an information security framework?
A. Recent audit findings
B. Implementation cost
C. Risk appetite
D. Available skills
Answer: (SHOW ANSWER)
Risk appetite (C) best informs the design of an information security framework because it defines the level of risk the organization is willing to accept in pursuit of its objectives. CISM stresses that security frameworks, policies, and control structures must be aligned with business risk tolerance to avoid over- or under- protection. Audit findings (A) highlight gaps, cost (B) affects feasibility, and available skills (D) influence implementation-but none define the strategic level of protection required. Risk appetite ensures that the framework supports business goals, prioritizes resources appropriately, and provides consistent guidance for decision-making across the organization. References: ISACA CISM Review Manual (Governance-risk appetite, framework design); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 60
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:
Freecram.net
A. baseline security controls.
B. benchmarking security metrics.
C. security objectives.
D. cost-benefit analyses.
Answer: (SHOW ANSWER)
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address security objectives, which are derived from the business objectives and the risk assessment. Security objectives define the desired level of protection for the system and its data, and guide the selection of security controls in later phases. Baseline security controls are predefined sets of security requirements that apply to common types of systems or environments. Benchmarking security metrics is a process of comparing the performance of security processes or controls against a standard or best practice. Cost-benefit analyses are used to evaluate the feasibility and effectiveness of security controls, and are usually performed in the acquisition/development phase or the implementation phase of the SDLC. References = CISM Review Manual, 16th Edition, page 1021; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 772 Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 61
Which of the following provides an information security manager with the MOST useful information on new threats and emerging risks that could impact business objectives?

A. External audit report
B. Internal threat analysis report
C. Industry threat intelligence report
D. Internal vulnerability assessment report
Answer: (SHOW ANSWER)
An industry threat intelligence report (C) provides the most useful insight into new and emerging threats because it aggregates intelligence across organizations, sectors, and geographies. CISM emphasizes the importance of understanding the external threat landscape to anticipate risks that may not yet be visible internally. Audit reports (A) and vulnerability assessments (D) are retrospective and organization-specific.
Internal threat analysis (B) focuses on known issues rather than emerging trends. Threat intelligence supports proactive risk identification and helps align security strategy with evolving business risks.
References: ISACA CISM Review Manual (Risk management-threat intelligence, emerging risk identification); CISM Exam Content Outline (Domain 1).

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 62
An organization is experiencing a sharp increase in incidents related to phishing messages. The root cause is an outdated email filtering system that is no longer supported by the vendor. Which of the following should be the information security manager's FIRST course of action?
A. Reinforce security awareness practices for end users.
B. Temporarily outsource the email system to a cloud provider.
C. Develop a business case to replace the system.
D. Monitor outgoing traffic on the firewall.
Answer: (SHOW ANSWER)
Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.
References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics." Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages." Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

NEW QUESTION: 63
Which of the following is the BEST way to build a risk-aware culture?
A. Periodically change risk awareness messages.
B. Periodically test compliance with security controls.
C. Establish a channel for staff to report risks.
D. Ensure that threats are documented and communicated in a timely manner.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following BEST describes a buffer overflow?
A. A function is carried out with more data than the function can handle
B. A program contains a hidden and unintended function that presents a security risk
C. Malicious code designed to interfere with normal operations
D. A type of covert channel that captures data
Answer: (SHOW ANSWER)
A buffer overflow is a software coding error or vulnerability that occurs when a function is carried out with more data than the function can handle, resulting in adjacent memory locations being overwritten or corrupted by the excess data1. A program contains a hidden and unintended function that presents a security risk is not a buffer overflow, but rather a backdoor2. Malicious code designed to interfere with normal operations is not a buffer overflow, but rather malware3. A type of covert channel that captures data is not a buffer overflow, but rather a keylogger.
References: 1 https://www.fortinet.com/resources/cyberglossary/buffer- overflow 2 https://www.fortinet.com/resources/cyberglossary/backdoor 3 https://www.fortinet.com/resources/cyberglossary/malware https://www.fortinet.com/resources/cyberglossary/keylogger

NEW QUESTION: 65
An information security manager wants to document requirements detailing the minimum security controls required for user workstations. Which of the following resources would be MOST appropriate for this purposed?
A. Guidelines
B. Policies

C. Procedures
D. Standards
Answer: (SHOW ANSWER)
Standards are detailed statements of the minimum requirements for hardware, software, or security configurations. They are used to define the minimum security controls required for user workstations. References = CISM Review Manual, 16th Edition, page 69.

NEW QUESTION: 66
Which of the following is the MOST critical input to developing policies, standards, and procedures to secure information assets?
A. Vulnerability assessment
B. Regulatory requirements
C. Industry best practices
D. Enterprise goals
Answer: (SHOW ANSWER)
Enterprise goals are the most critical input because security policies must align with and support the organization's objectives and mission. Policies that do not align with enterprise goals are less likely to gain management support and may not effectively protect key assets.
"Information security must support enterprise goals and objectives to ensure alignment with the broader business strategy."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Alignment with Business Goals and Objectives ISACA's CISM questions reiterate that alignment with enterprise goals is essential for policy effectiveness.

NEW QUESTION: 67
An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?
A. Control owner responses based on a root cause analysis
B. The impact of noncompliance on the organization's risk profile
C. A noncompliance report to initiate remediation activities
D. A business case for transferring the risk
Answer: (SHOW ANSWER)
The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions.
Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.
References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process." CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

NEW QUESTION: 68
An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?
A. Perform a vulnerability assessment
B. Conduct an internal audit
C. Conduct penetration testing
D. Prepare compensating controls
Answer: (SHOW ANSWER)
Penetration testing simulates real-world attacks to identify any remaining exploitable vulnerabilities after controls are implemented. It validates that mitigation has been successful from an attacker's perspective.
"Penetration testing is essential to verify the effectiveness of remediation efforts and ensure vulnerabilities can no longer be exploited."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Security Testing and Evaluation* Vulnerability assessments and audits are valuable, but pen testing provides practical assurance.

NEW QUESTION: 69
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).
Answer: (SHOW ANSWER)
Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified

as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.
Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented. References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

NEW QUESTION: 70

Which of the following considerations is MOST important when selecting a third-party intrusion detection system (IDS) vendor?

Freecram.net

A. The vendor's proposal allows for contract modification during technology refresh cycles.
B. The vendor's proposal requires the provider to have a business continuity plan (BCP).
C. The vendor's proposal allows for escrow in the event the third party goes out of business.
D. The vendor's proposal aligns with the objectives of the organization.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71

A project team member notifies the information security manager of a potential security risk that has not been included in the risk register. Which of the following should the information security manager do FIRST?
A. Add the risk to the risk register.
B. Analyze the identified risk.
C. Implement compensating controls.
D. Prepare a risk mitigation plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 72

An information security team has confirmed that threat actors are taking advantage of a newly announced critical vulnerability within an application. Which of the following should be done FIRST?

A. Install additional application controls.
B. Notify senior management.
C. Invoke the incident response plan.
D. Prevent access to the application.
Answer: (SHOW ANSWER)
According to the NIST SP 800-61 Computer Security Incident Handling Guide1, the first step in responding to a cybersecurity incident is to invoke the incident response plan (IRP), which is a written document that defines the roles, responsibilities, and procedures for dealing with a confirmed or suspected security breach1. The IRP helps the organization to prepare for, detect, analyze, contain, eradicate, recover from, and learn from incidents1. Invoking the IRP ensures that the right personnel and resources are mobilized to effectively deal with the threat and minimize the impact.
References = 1: NIST SP 800-61: 1. Introduction1

NEW QUESTION: 73
Which of the following change management procedures is MOST likely to cause concern to the information security manager?
A. Fallback processes are tested the weekend before changes are made
B. Users are not notified of scheduled system changes
C. A manual rather than an automated process is used to compare program versions.
D. The development manager migrates programs into production
Answer: D (LEAVE A REPLY)
The change management procedure that is MOST likely to cause concern to the information security manager is the development manager migrating programs into production, because it involves a high-risk activity that could compromise the confidentiality, integrity, and availability of the information systems and data.
Migrating programs into production without proper testing, validation, and approval could introduce errors, vulnerabilities, or conflicts that could affect the performance, functionality, or security of the systems. Fallback processes are tested the weekend before changes are made, users are not notified of scheduled system changes, and a manual rather than an automated process is used to compare program versions are all acceptable change management procedures that do not pose significant risks to the information security manager. References = CISM Review Manual, 16th Edition, page 3121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1522

NEW QUESTION: 74
During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption, unauthorized alterations, and errors?
A. Configuration management
B. Password management
C. Change management

D. Version management

Answer: (SHOW ANSWER)

Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.

References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION: 75

Which of the following is the MOST beneficial outcome of testing an incident response plan?

A. The response includes escalation to senior management

B. Incident response time is improved

C. The plan is enhanced to reflect the findings of the test

D. Test plan results are documented

Answer: (SHOW ANSWER)

The correct answer is C because the most beneficial outcome of testing an incident response plan is using the findings to improve the plan. Testing is not performed only to confirm that a plan exists; it is performed to identify weaknesses, validate assumptions, clarify roles, improve communication, and strengthen response capability. When the plan is enhanced based on test findings, the organization gains lasting value and improves preparedness for future incidents. Improved response time is a valuable result, but it usually occurs because the plan, procedures, training, or coordination have been improved after testing. Escalation to senior management may be appropriate for certain incidents, but it is not always required and is not the main benefit of testing. Documenting test results is necessary for accountability and lessons learned, but documentation alone does not improve response capability unless corrective actions are taken. CISM incident management emphasizes testing, lessons learned, continuous improvement, and plan maintenance. Therefore, enhancing the plan based on test findings is the best answer. Reference: CISM Information Security Incident Management; incident response testing, lessons learned, plan maintenance, and continuous improvement principles.

NEW QUESTION: 76

Which of the following is the BEST course of action when an information security manager identifies that systems are vulnerable to emerging threats?

A. Frequently update systems and monitor the threat landscape.

B. Monitor the network containing the affected systems for malicious traffic.

C. Increase awareness of the threats among employees who work with the systems.

D. Notify senior management and key stakeholders of the threats.

Answer: (SHOW ANSWER)

The best course of action when an information security manager identifies that systems are vulnerable to emerging threats is to frequently update systems and monitor the threat landscape, as this will help to reduce the exposure and impact of the threats, and enable timely detection and response. Updating systems involves applying patches, fixing vulnerabilities, and implementing security controls. Monitoring the threat landscape involves collecting and analyzing threat intelligence, identifying new attack vectors and techniques, and assessing the risk and impact of the threats.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2211; State of Cybersecurity 2023: Navigating Current and Emerging Threats2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 77
Several months after the installation of a new firewall with intrusion prevention features to block malicious activity, a breach was discovered that came in through the firewall shortly after installation. This breach could have been detected earlier by implementing firewall:
A. log monitoring
B. application awareness
C. web surfing controls
D. packet filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Application data integrity risk is MOST directly addressed by a design that includes:
A. reconciliation routines such as checksums, hash totals, and record counts.
B. strict application of an authorized data dictionary.
C. application log requirements such as field-level audit trails and user activity logs.
D. access control technologies such as role-based entitlements.
Answer: (SHOW ANSWER)
Reconciliation routines are methods to verify the integrity of data by comparing the input and output of a process or a system. They can detect errors, omissions, duplications or unauthorized modifications of data. They are more directly related to data integrity than the other options, which

are more concerned with data definition, logging or access control. References = CISM Review Manual, 16th Edition, Chapter 3, Section 3.4.21

NEW QUESTION: 79
An employee clicked on a malicious link in an email that resulted in compromising company data. What is the BEST way to mitigate this risk in the future?
A. Conduct phishing awareness training.
B. Implement disciplinary procedures.
C. Establish an acceptable use policy.
D. Assess and update spam filtering rules.
Answer: (SHOW ANSWER)
Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

NEW QUESTION: 80
Which of the following is the MOST effective way to identify changes in an information security environment?
Freecram.net
A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring
Answer: (SHOW ANSWER)
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-
1371, page 1, section 1.1.

NEW QUESTION: 81
Which of the following is MOST important to ensure the alignment of an information security program with the organizational strategy?
A. Approval from senior management
B. Identification of business-specific risk factors
C. Adoption of an industry recognized framework
D. Benchmarking against industry peers

Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following is the BEST strategy when determining an organization's approach to risk treatment?
A. Advancing the maturity of existing controls based on risk tolerance
B. Prioritizing controls that directly mitigate the organization's most critical risks
C. Implementing risk mitigation controls that are considered quick wins
D. Implementing a one-size-fits-all set of controls across all organizational units
Answer: (SHOW ANSWER)
The best strategy for risk treatment is to prioritize controls that directly mitigate the organization's most critical risks. This aligns with a risk-based approach, where limited resources are directed toward areas with the highest business impact.
"Effective risk treatment involves prioritizing actions that address the most critical risks to the organization, considering impact and likelihood."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Advancing maturity or applying quick wins may help, but they are not as strategic or impactful as targeting top-priority risks.

NEW QUESTION: 83
Which of the following is the PRIMARY objective of incident triage?
A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats
Answer: (SHOW ANSWER)
The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization's information security.
Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization's assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident. References = CISM Certified Information Security Manager Study Guide, Chapter 8:

Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; Critical Incident Stress Management - National Interagency Fire Center3; Critical Incident Stress Management - US Forest Service4

NEW QUESTION: 84
Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?
A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes
C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards
Answer: (SHOW ANSWER)
A service provider is a third-party supplier that provides IT services or products to an organization. A service provider should comply with the organization's information security requirements, such as policies, standards, procedures, and controls, to ensure the confidentiality, integrity, and availability of the organization's data and systems. The best way to provide an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements is to have the ability to audit the third-party supplier's IT systems and processes. An audit is a systematic and independent examination of evidence to determine the degree of conformity to predetermined criteria. An audit can verify the effectiveness and efficiency of the service provider's security controls, identify any gaps or weaknesses, and provide recommendations for improvement. An audit can also ensure that the service provider adheres to the contractual obligations and service level agreements (SLAs) with the organization. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a live demonstration of the third-party supplier's security capabilities may not be comprehensive, objective, or reliable. A live demonstration may only show the positive aspects of the service provider's security, but not reveal any hidden or potential issues. A live demonstration may also be subject to manipulation or deception by the service provider.
Option C is not the best answer because third-party security control self-assessment (CSA) results may not be accurate, complete, or consistent. A self-assessment is a process where the service provider evaluates its own security controls against a set of criteria or standards. A self-assessment may be biased, subjective, or incomplete, as the service provider may not disclose or report all the relevant information or issues. A self- assessment may also vary in quality and scope depending on the service provider's expertise, resources, and methodology.
Option D is not the best answer because an independent review report indicating compliance with industry standards may not be sufficient or specific for the organization's information security requirements. An independent review is a process where an external party evaluates the service provider's security controls against a set of industry standards or best practices, such as ISO/IEC 27001, NIST CSF, PCI DSS, etc. An independent review report may provide a general overview of the service provider's security posture, but not address the organization's unique or specific

security needs, risks, or expectations. An independent review report may also be outdated, limited, or generic, as the industry standards or best practices may not reflect the current or emerging security threats or trends. References = CISM Review Manual 15th Edition1, pages 257-
258; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 301.
An independent review report indicating compliance with industry standards BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

NEW QUESTION: 85
Which of the following is the MOST important consideration when planning to implement artificial intelligence to enhance an organization's vulnerability and control deficiency analysis capabilities?
A. The alignment of artificial intelligence tools with the organization's existing security policies
B. The adaptability and scalability of artificial intelligence tools
C. The interoperability of artificial intelligence tools with the existing security infrastructure and technologies
D. The artificial intelligence-related training requirements for existing security staff
Answer: (SHOW ANSWER)
The correct answer is C because artificial intelligence tools used for vulnerability and control deficiency analysis must integrate effectively with the organization's existing security infrastructure and technologies.
Such tools usually rely on data from vulnerability scanners, configuration management systems, SIEM platforms, endpoint tools, asset inventories, ticketing systems, cloud platforms, and control monitoring solutions. If interoperability is weak, the artificial intelligence capability may receive incomplete, inaccurate, delayed, or inconsistent data, reducing the value of analysis and decision support. Alignment with policies is important, but policy alignment alone will not ensure that the tool can function effectively. Adaptability and scalability are also useful, especially as environments grow, but they are secondary to the tool's ability to connect with current systems. Training requirements are important for adoption, but training cannot compensate for poor technical integration. From a CISM program management perspective, new security capabilities should be planned to support existing processes, technologies, reporting, and risk management objectives. Therefore, interoperability is the most important consideration.
Reference: CISM Information Security Program Development and Management; security technology integration, vulnerability management, control monitoring, and program enablement principles.

NEW QUESTION: 86
An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?
A. Determine which country's information security regulations will be used.
B. Merge the two existing information security programs.
C. Apply the existing information security program to the acquired company.
D. Evaluate the information security laws that apply to the acquired company.
Answer: (SHOW ANSWER)
The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

NEW QUESTION: 87
Which of the following control types should be considered FIRST for aligning employee behavior with an organization's information security objectives?
A. Technical security controls
B. Access security controls
C. Administrative security controls
D. Physical security controls
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following is the BEST way to reduce the risk associated with a bring your own device (BYOD) program?
A. Require employees to install an effective anti-malware app.
B. Implement a mobile device management (MDM) solution.
C. Implement a mobile device policy and standard.
D. Provide employee training on secure mobile device practices.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:
A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.

D. right to audit is included in the service level agreement (SLA).

Answer: (SHOW ANSWER)

= To confirm that a third-party provider complies with an organization's information security requirements, it is most important to ensure that the right to audit is included in the service level agreement (SLA), which is a contract that defines the scope, quality, and terms of the services that the third-party provider delivers to the organization. The right to audit is a clause that grants the organization the authority and opportunity to inspect and verify the third-party provider's security policies, procedures, controls, and performance, either by itself or by an independent auditor, at any time during the contract period or after a security incident. The right to audit can help to ensure that the third-party provider adheres to the organization's information security requirements, as well as to the legal and regulatory standards and obligations, and that the organization can monitor and measure the security risks and issues that arise from the outsourcing relationship. The right to audit can also help to identify and address any gaps, weaknesses, or errors that could compromise the security of the information assets and systems that are shared, stored, or processed by the third-party provider, and to provide feedback and recommendations for improvement and optimization of the security posture and performance. Security metrics, contract clauses, and the information security policy of the third-party provider are all important elements of ensuring the compliance of the third-party provider with the organization's information security requirements, but they are not the most important ones. Security metrics are quantitative and qualitative measures that indicate the effectiveness and efficiency of the security controls and processes that the third-party provider implements and reports to the organization, such as the number of security incidents, the time to resolve them, the level of customer satisfaction, or the compliance rate. Security metrics can help to evaluate and compare the security performance and outcomes of the third-party provider, as well as to identify and address any deviations or discrepancies from the expected or agreed levels. Contract clauses are legal and contractual terms and conditions that bind the third-party provider to the organization's information security requirements, such as the confidentiality, integrity, and availability of the information assets and systems, the roles and responsibilities of the parties, the liabilities and penalties for breach or violation, or the dispute resolution mechanisms. Contract clauses can help to enforce and protect the organization's information security interests and rights, as well as to prevent or resolve any conflicts or issues that arise from the outsourcing relationship. The information security policy of the third-party provider is a document that defines and communicates the third-party provider's security vision, mission, objectives, and principles, as well as the security roles, responsibilities, and rules that apply to the third-party provider's staff, customers, and partners. The information security policy of the third-party provider can help to ensure that the third-party provider has a clear and consistent security direction and guidance, as well as to align and integrate the third- party provider's security practices and culture with the organization's security expectations and requirements. References = CISM Review Manual 15th Edition, pages 57-581; CISM Practice Quiz, question
1662

NEW QUESTION: 90

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

Freecram.net

A. Perform a risk assessment

B. Perform a gap analysis

C. Review information security policies

D. Review the state of security awareness

Answer: (SHOW ANSWER)

During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.

"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence

ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

NEW QUESTION: 91

Which of the following is the MOST useful input for an information security manager when updating the organization's security policy?

A. Security team capabilities

B. Industry benchmarks

C. Risk appetite

D. Vulnerability scan results

Answer: (SHOW ANSWER)

The correct answer is C because information security policy should reflect the organization's risk appetite, business objectives, and governance direction. Risk appetite defines the amount and type of risk the organization is willing to accept in pursuit of its objectives. Policies establish management's expectations for protecting information assets, so they must be aligned with the level of risk the organization is prepared to tolerate. Security team capabilities may influence implementation planning, but they should not be the primary driver of policy. Industry benchmarks can help compare practices, but they may not reflect the organization's specific business context or risk tolerance. Vulnerability scan results identify technical weaknesses, but they are too narrow to guide enterprise-level policy updates. In CISM, policies are governance instruments that communicate required behavior and control expectations. Therefore, risk appetite is the most useful input because it ensures the updated policy supports business priorities and risk-based decision-making.

Reference: CISM Information Security Governance; policy management, risk appetite, enterprise objectives, and governance alignment principles.

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 92
Which of the following is the MOST cost-effective method for assessing an organization's incident response capabilities?
A. Tabletop exercise
B. Senior management interview
C. Penetration testing
D. Third-party assessment
Answer: (SHOW ANSWER)
The correct answer is A because a tabletop exercise is a low-cost and effective way to assess incident response capabilities. It allows participants to walk through a simulated incident scenario and evaluate roles, responsibilities, escalation paths, communication procedures, decision-making, and coordination without disrupting production systems. A tabletop exercise can identify weaknesses in the incident response plan, improve readiness, and increase participant familiarity with response procedures. Senior management interviews may provide insight into governance awareness, but they do not test operational response capability. Penetration testing can identify vulnerabilities and may trigger response processes, but it is more expensive and focused on technical exposure rather than full incident response capability. A third-party assessment can be valuable, but it is usually more costly than an internal tabletop exercise. CISM incident management emphasizes regular testing, lessons learned, and continuous improvement. Because tabletop exercises provide practical assessment value with relatively low cost and low operational risk, they are the most cost-effective method.
Reference: CISM Information Security Incident Management; incident response testing, tabletop exercises, preparedness, and continuous improvement principles.

NEW QUESTION: 93
The fundamental purpose of establishing security metrics is to:
A. increase return on investment (ROI)
B. provide feedback on control effectiveness
C. adopt security best practices
D. establish security benchmarks
Answer: (SHOW ANSWER)

The fundamental purpose of establishing security metrics is to provide feedback on the effectiveness of the information security controls and processes. Security metrics are quantitative or qualitative measures that indicate how well the organization is achieving its security objectives and goals. Security metrics can help the information security manager to monitor, evaluate, and improve the performance of the information security program, as well as to identify gaps, weaknesses, and areas for improvement. Security metrics can also help the organization to demonstrate compliance with internal and external standards, regulations, and best practices. Increasing return on investment (ROI), adopting security best practices, and establishing security benchmarks are possible outcomes or benefits of using security metrics, but they are not the fundamental purpose of establishing them. References = CISM Review Manual, 16th Edition, pages 46-471; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 642
Learn more:
1. isaca.org2. amazon.com3. gov.uk
Security metrics are used to measure the effectiveness of controls and evaluate the overall security posture of an organization. This feedback provides an understanding of the progress made towards achieving security objectives and allows organizations to make necessary adjustments.

NEW QUESTION: 94
Threat and vulnerability assessments are important PRIMARILY because they are:
A. used to establish security investments
B. the basis for setting control objectives.
C. elements of the organization's security posture.
D. needed to estimate risk.
Answer: (SHOW ANSWER)
Threat and vulnerability assessments are important primarily because they are the basis for setting control objectives. Control objectives are the desired outcomes of implementing security controls, and they should be aligned with the organization's risk appetite and business objectives. Threat and vulnerability assessments help to identify the potential sources and impacts of security incidents, and to prioritize the mitigation actions based on the likelihood and severity of the risks. By conducting threat and vulnerability assessments, the organization can establish the appropriate level and type of security controls to protect its information assets and reduce the residual risk to an acceptable level. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Threat and vulnerability assessments are important PRIMARILY because they are the basis for setting control objectives. Control objectives are the desired outcomes or goals of implementing security controls in an information system. They are derived from the risk assessment process, which identifies and evaluates the threats and vulnerabilities that could affect the system's

confidentiality, integrity and availability. By conducting threat and vulnerability assessments, an organization can determine the level of risk it faces and establish the appropriate control objectives to mitigate those risks.

NEW QUESTION: 95
Which of the following BEST enables the restoration of operations after a limited ransomware incident occurs?
A. Root cause analysis
B. Reliable image backups
C. Impact assessment
D. Documented eradication procedures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
An incident management team leader sends out a notification that the organization has successfully recovered from a cyberattack. Which of the following should be done NEXT?
A. Prepare an executive summary for senior management
B. Gather feedback on business impact
C. Conduct a meeting to capture lessons learned.
D. Secure and preserve digital evidence for analysis.
Answer: C (LEAVE A REPLY)
Conducting a meeting to capture lessons learned is the next step after an incident management team leader sends out a notification that the organization has successfully recovered from a cyberattack because it helps to identify the strengths and weaknesses of the current incident response plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Preparing an executive summary for senior management is not the next step, but rather a subsequent step that involves reporting the incident details, impact, and resolution to the senior management. Gathering feedback on business impact is not the next step, but rather a concurrent step that involves assessing the extent and severity of the damage or disruption caused by the incident.
Securing and preserving digital evidence for analysis is not the next step, but rather a previous step that involves collecting and documenting the relevant data or artifacts related to the incident.
References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 97

Which of the following is MOST important to convey to employees in building a security risk-aware culture?

A. Personal information requires different security controls than sensitive information.

B. Employee access should be based on the principle of least privilege.

C. Understanding an information asset's value is critical to risk management.

D. The responsibility for security rests with all employees.

Answer: (SHOW ANSWER)

= The most important message to convey to employees in building a security risk-aware culture is that the responsibility for security rests with all employees, not just the information security function or the management. A security risk-aware culture is a collective mindset of the people in the organization working every day to protect the enterprise and its information assets from internal and external threats. A security risk- aware culture requires the workforce to know the security risks and the processes for avoiding or mitigating them, and to make thoughtful decisions that align with security policies and standards. A security risk-aware culture also incorporates a broader corporate culture of day-to-day actions that encourage employees to report security incidents, share security best practices, and participate in security awareness and training programs.

A security risk-aware culture helps to reduce the human factor that causes 90 percent of all cyberattacks, and to offset the impact of corrupted or lost data, decreased revenue, regulatory fines, and reputational damage. A security risk-aware culture turns people from assets that must be protected into assets that actively contribute to the cybersecurity and risk management posture and elevate security to being a business enabler rather than a business impediment123.

Personal information requires different security controls than sensitive information is a true statement, but it is not the most important message to convey to employees in building a security risk-aware culture. Personal information is any information that can identify or relate to a natural person, such as name, address, email, phone number, social security number, etc. Sensitive information is any information that is confidential, proprietary, or has a high value or impact to the organization, such as trade secrets, financial data, customer data, intellectual property, etc. Different types of information may have different legal, regulatory, contractual, or ethical obligations to protect them from unauthorized access, use, disclosure, modification, or destruction. Therefore, different security controls may be applied to personal and sensitive information based on their classification, such as encryption, access control, retention, disposal, etc. However, this message does not address the broader concept of security risk-aware culture, which is not limited to information classification and protection, but also encompasses the behaviors, attitudes, and values of the employees towards security.

Employee access should be based on the principle of least privilege is a good practice, but it is not the most important message to convey to employees in building a security risk-aware culture. The principle of least privilege states that users should only have the minimum level of access and permissions that are necessary to perform their job functions, and no more. This principle helps to reduce the risk of unauthorized or inappropriate actions, such as data leakage, fraud, sabotage, etc., by limiting the exposure and impact of user activities. However, this message

does not capture the essence of security risk-aware culture, which is not only about access control, but also about the awareness, understanding, and commitment of the employees to security.
Understanding an information asset's value is critical to risk management is a valid point, but it is not the most important message to convey to employees in building a security risk-aware culture. Understanding an information asset's value is essential to determine the potential impact and likelihood of a security risk, and to prioritize the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
However, this message does not reflect the holistic nature of security risk-aware culture, which is not only about risk assessment, but also about risk communication, risk treatment, and risk monitoring. References = Building a Culture of Security - ISACA2 The Risk-Conscious, Security-Aware Culture: The Forgotten Critical Security Control - Cisco3 CISM ITEM DEVELOPMENT GUIDE - ISACA4

NEW QUESTION: 98
An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?
A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.
Answer: (SHOW ANSWER)
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION: 99
Which of the following should be of GREATEST concern regarding an organization's security controls?
A. Some controls are performing outside of an acceptable range.
B. No key control indicators (KCIs) have been implemented.
C. Control ownership has not been updated.

D. Control gap analysis is outdated.

Answer: (SHOW ANSWER)

Key Control Indicators (KCIs) are essential to measuring the effectiveness and performance of security controls. Without them:

The organization cannot assess if controls are working as intended

It's difficult to demonstrate due diligence

Risks may go unnoticed

While other answers point to operational concerns, the complete absence of KCIs presents a critical governance gap that compromises the organization's ability to monitor and manage control health.

"KCIs provide actionable metrics that support proactive control management and are fundamental to governance and assurance."

- CISM Review Manual 15th Edition, Chapter 1: Governance Metrics and Reporting*

NEW QUESTION: 100

An organization wants to outsource all non-core IT functions to external service providers. Which of the following is MOST important to include in the procurement process to maintain the desired security level?

Freecram.net

A. Conducting industry benchmarking to determine vendor alignment with the business

B. Performing a risk assessment to enable selection of appropriate controls

C. Conducting a security audit to identify gaps for remediation

D. Performing a business impact analysis to minimize security impact

Answer: (SHOW ANSWER)

The correct answer is B because outsourcing IT functions introduces third-party risk, and the organization must perform a risk assessment during procurement to identify the controls required to maintain the desired security level. A risk assessment helps determine data sensitivity, service criticality, regulatory requirements, access needs, vendor dependencies, contractual controls, monitoring requirements, and residual risk. Industry benchmarking may provide useful comparison, but it does not identify the organization's specific outsourcing risks. A security audit may be useful after vendor selection or as part of due diligence, but the first procurement need is to understand risk and define appropriate security requirements. A business impact analysis is valuable for continuity planning, but it is not the main activity for selecting security controls in outsourcing. CISM emphasizes that third-party arrangements should be governed through risk assessment, due diligence, contracts, monitoring, and control requirements. Therefore, risk assessment is the most important procurement activity.

Reference: CISM Information Risk Management; third-party risk management, outsourcing, procurement controls, due diligence, and vendor risk assessment principles.

NEW QUESTION: 101

Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?

A. Security information and event management (SIEM)
B. Extended detection and response (XDR)
C. Endpoint detection and response (EDR)
D. Network intrusion detection system (NIDS)
Answer: A (LEAVE A REPLY)
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

NEW QUESTION: 102
Which of the following is the BEST way to obtain support for a new organization-wide information security program?
A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.
Answer: (SHOW ANSWER)
= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by:
Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.
Establishing roles and responsibilities for the security program and ensuring accountability and ownership.
Securing adequate resources and budget for the security program and allocating them appropriately.
Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.
Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.
Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security

program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges.
Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.
Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization. An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.
Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication, confusion, or conflict. However, a RACI chart does not ensure the support or commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders.
References = CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112
Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition
- ISACA1
Information Security Strategy: The Key to Success - ISACA2
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

NEW QUESTION: 103
What type of control is being implemented when a security information and event management (SIEM) system is installed?
A. Preventive
B. Deterrent
C. Detective
D. Corrective
Answer: (SHOW ANSWER)
A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. References: https://www.
isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org
/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 104
Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?
A. Alignment with industry benchmarks
B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget
Answer: (SHOW ANSWER)
The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

NEW QUESTION: 105
Which of the following should be the FIRST step in developing an information security strategy?
A. Determine acceptable levels of information security risk
B. Create a roadmap to identify security baselines and controls

C. Perform a gap analysis based on the current state
D. Identify key stakeholders to champion information security
Answer: (SHOW ANSWER)
The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them. Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

NEW QUESTION: 106
Which of the following should be the PRIMARY goal of information security?
A. Data governance
B. Business alignment
C. Information management
D. Regulatory compliance
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 107
Which of the following is the MOST important criterion when deciding whether to accept residual risk?
A. Cost of replacing the asset
B. Cost of additional mitigation
C. Annual loss expectancy (ALE)
D. Annual rate of occurrence
Answer: (SHOW ANSWER)
= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one-year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk

event occurring within a one-year period, and SLE is the estimated cost of a single occurrence of a risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance. Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
22, page 242

NEW QUESTION: 108
Which of the following is the BEST reason to implement a comprehensive information security management system?
A. To ensure continuous alignment with the organizational strategy
B. To gain senior management support for the information security program
C. To support identification of key risk indicators (KRIs)
D. To facilitate compliance with external regulatory requirements
Answer: A (LEAVE A REPLY)
According to the CISM Review Manual, 15th Edition, the primary objective of an information security management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks.
References = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

NEW QUESTION: 109
An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?
A. Security requirements are included in the vendor contract
B. External security audit results are reviewed.
C. Service level agreements (SLAs) meet operational standards.
D. Business continuity contingency planning is provided
Answer: (SHOW ANSWER)
Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.

References:
https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations
https://www.sciencedirect.com/science/article/pii/S0378720616302166

NEW QUESTION: 110

Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?

Freecram.net

A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk
Answer: (SHOW ANSWER)
Communicating the residual risk is the best way to facilitate an information security manager's efforts to obtain senior management commitment for an information security program. The residual risk is the level of risk that remains after applying the security controls and mitigation measures. The residual risk reflects the effectiveness and efficiency of the information security program, as well as the potential impact and exposure of the organization. The information security manager should communicate the residual risk to the senior management in a clear, concise, and relevant manner, using quantitative or qualitative methods, such as risk matrices, heat maps, dashboards, or reports. The communication of the residual risk should also include the comparison with the inherent risk, which is the level of risk before applying any security controls, and the risk appetite, which is the level of risk that the organization is willing to accept. The communication of the residual risk should help the senior management to understand the value and performance of the information security program, as well as the need and justification for further investment or improvement. Presenting evidence of inherent risk, reporting the security maturity level, and presenting compliance requirements are all important aspects of the information security program, but they are not the best ways to obtain senior management commitment. These aspects may not directly demonstrate the benefits or outcomes of the information security program, or they may not align with the business objectives or priorities of the organization. For example, presenting evidence of inherent risk may show the potential threats and vulnerabilities that the organization faces, but it may not indicate how the information security program addresses or reduces them. Reporting the security maturity level may show the progress and status of the information security program, but it may not relate to the risk level or the business impact. Presenting compliance requirements may show the legal or regulatory obligations that the organization must fulfill, but it may not reflect the actual security needs or goals of the organization. Therefore, communicating the residual risk is the best way to obtain senior management commitment for an information security program, as it shows the results and value of the information security program for the organization. References = CISM Review Manual 2023, page 41 1; CISM Practice Quiz 2

NEW QUESTION: 111
Predetermined containment methods to be used in a cybersecurity incident response should be based PRIMARILY on the:
A. number of impacted users.
B. capability of incident handlers.
C. type of confirmed incident.
D. predicted incident duration.
Answer: (SHOW ANSWER)
According to the NIST SP 800-61 Computer Security Incident Handling Guide, the type of confirmed incident is one of the most important criteria for choosing a containment strategy, as different types of incidents may require different levels of urgency, scope, and impact1. For example, a denial-of-service attack may require a different containment strategy than a ransomware attack or a data breach.
References = 1: NIST SP 800-61: 3.1. Choosing a Containment Strategy2

NEW QUESTION: 112
Which of the following is the BEST method to protect the confidentiality of data transmitted over the Internet?
A. Network address translation (NAT)
B. Message hashing
C. Transport Layer Security (TLS)
D. Multi-factor authentication
Answer: C (LEAVE A REPLY)
Transport Layer Security (TLS) is a protocol that provides encryption, authentication, and integrity for data transmitted over the Internet. TLS protects the confidentiality of data by encrypting it before sending it and decrypting it after receiving it. TLS also verifies the identity of the communicating parties by using certificates and prevents data tampering by using message authentication codes. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.3.2.11

NEW QUESTION: 113
Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?
A. Enforce the local regulation.
B. Obtain legal guidance.
C. Enforce the organization's information security policy.
D. Obtain an independent assessment of the regulation.
Answer: (SHOW ANSWER)
The information security manager should first obtain legal guidance when there is a conflict between the organization's information security policy and a local regulation, because this will help to understand the implications and consequences of the conflict, and to identify the possible

options and solutions for resolving it. The information security manager should also consult with the relevant stakeholders, such as senior management, business owners, and information owners, to determine the best course of action that aligns with the organization's objectives, risk appetite, and compliance obligations. Enforcing the local regulation or the organization's information security policy without legal guidance may expose the organization to legal liabilities, security risks, or operational disruptions. Obtaining an independent assessment of the regulation may be helpful, but it is not the first step to take.
References = CISM Review Manual, 16th Edition, page 691; A Guide to ISACA CISM Domains & Domain
1: Information Security Governance2

NEW QUESTION: 114
Which of the following is the MOST effective way to increase security awareness in an organization?
A. Implement regularly scheduled information security audits.
B. Require signed acknowledgment of information security policies.
C. Conduct periodic simulated phishing exercises.
D. Include information security requirements in job descriptions.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?
A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan
Answer: (SHOW ANSWER)
The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type, scope, and complexity of the forensic investigation, the legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the

accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The existence of the provider's incident response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any security incidents that may affect the forensic service or the organization. The existence of the provider's incident response plan can help to protect the confidentiality, integrity, and availability of the forensic evidence or data, as well as to comply with the legal and contractual obligations. However, the existence of the provider's incident response plan does not confirm that the provider has the technical capabilities to execute the forensic service competently and ethically12.
References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance - ISACA2

NEW QUESTION: 116
Which of the following should be an information security manager's PRIMARY concern when an organization is expanding business to a new country?
A. Changes in IT infrastructure
B. Cultural differences in the new country
C. Ability to gather customer data
D. Compliance with local regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?
A. Chief information security officer (CISO)
B. Information security steering committee
C. Enterprise risk committee
D. Data privacy officer (DPO)
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Of the following, who is accountable for ensuring the incident response plan is tested?
A. Business process owner
B. Business continuity manager
C. Incident response team members
D. Information security manager
Answer: (SHOW ANSWER)
The correct answer is D because the information security manager is accountable for ensuring that the incident response capability is maintained, tested, and improved. Incident response plans must be tested periodically to confirm that roles, escalation paths, communication procedures, containment steps, and recovery coordination work as intended. Business process owners are responsible for business processes and may participate in tests, especially where business impact is involved, but they are not normally accountable for the information security incident response plan itself. The business continuity manager may be accountable for business continuity or disaster recovery exercises, but this question specifically refers to incident response. Incident response team members perform response activities and participate in exercises, but accountability for ensuring the plan is tested belongs to the manager responsible for the incident management program. CISM emphasizes that information security management includes establishing, maintaining, testing, and improving incident management processes to reduce organizational impact when incidents occur.
Reference: CISM Information Security Incident Management; incident response planning, testing, accountability, and continuous improvement principles.

NEW QUESTION: 119
A security incident has been reported within an organization. When should an information security manager contact the information owner?
A. After the incident has been contained
B. After the incident has been mitigated
C. After the incident has been confirmed
D. After the potential incident has been logged
Answer: (SHOW ANSWER)
The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 120

Which of the following is PRIMARILY determined by asset classification?

A. Insurance coverage required for assets

B. Level of protection required for assets

C. Priority for asset replacement

D. Replacement cost of assets

Answer: (SHOW ANSWER)

Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. References = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

NEW QUESTION: 121

Which of the following should be the MOST important consideration when reviewing an information security strategy?

A. Recent security incidents

B. New business initiatives

C. Industry security standards

D. Internal audit findings

Answer: (SHOW ANSWER)

New business initiatives are the most important consideration, as security must align with business changes to effectively protect assets and support growth.

"The security strategy must be aligned with new business initiatives to ensure it continues to protect critical assets and support enterprise goals."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment* ISACA practice questions stress that aligning with new business initiatives ensures relevance and effectiveness.

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here:

https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122
An organization plans to implement a new e-commerce operation in a highly regulated market. Which of the following is MOST important to consider when updating the risk management strategy?
A. Strategy of industry peers
B. Outsourcing needs
C. Business culture
D. Compliance requirements
Answer: (SHOW ANSWER)
When operating in a highly regulated market, compliance requirements become paramount, as failure to comply can lead to severe legal penalties, financial losses, and reputational harm. According to the CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Task 2, understanding and addressing legal, regulatory, and contractual requirements is critical in risk management, especially in regulated environments. This ensures that the risk management strategy is aligned with mandatory regulations and industry standards. Other factors (such as outsourcing and business culture) are important, but compliance is the primary driver in highly regulated markets.
Reference:ISACA CISM Review Manual, 16th Edition, Page 120-122, "Legal, Regulatory and Contractual Requirements".

NEW QUESTION: 123
An organization has identified a weakness in the ability of its employees to identify and report cybersecurity incidents. Although training materials have been provided, employees show a lack of interest. Which of the following is the information security manager's BEST course of action?
A. Block network access until security awareness training is complete.
B. Conduct an enterprise cybersecurity risk assessment.
C. Obtain key stakeholder and leadership support.
D. Send an email mandating training for the employees.
Answer: (SHOW ANSWER)
Leadership support reinforces the importance of security awareness and motivates employees to engage with training.
"Security awareness programs are most effective when they have visible support from senior management, reinforcing their importance."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training*

NEW QUESTION: 124

An organization is outsourcing a business function to an external vendor. Which of the following BEST enables management to ensure the vendor continuously complies with security requirements stated in the master contract?

A. Organize a training program for the vendor on the organization's security requirements.

B. Conduct periodic reviews of the vendor's third-party accredited assessments.

C. Establish the right-to-audit security controls at the vendor site.

D. Conduct periodic re-approval of security clauses in the master contract.

Answer: (SHOW ANSWER)

The best way to ensure continuous compliance with security requirements is to conduct periodic reviews of the vendor's third-party accredited assessments (B). From a CISM governance and third-party risk management perspective, ongoing assurance is critical when business-critical functions are outsourced.

Independent third-party assessments (such as SOC reports or equivalent accredited reviews) provide objective, repeatable, and evidence-based validation that security controls are not only defined but are operating effectively over time.

Training programs (A) improve awareness but do not provide assurance of compliance. Establishing right-to- audit clauses (C) is an important contractual safeguard, but it is typically reactive or periodic, not a continuous monitoring mechanism. Re-approving contract clauses (D) ensures contractual relevance but does not validate actual control effectiveness.

CISM emphasizes that continuous vendor compliance is best achieved through independent assurance mechanisms integrated into ongoing vendor oversight, enabling management to monitor control effectiveness, identify emerging risks, and take timely corrective action. Periodic review of accredited third-party assessments supports governance transparency, accountability, and alignment with the organization's risk appetite.

References:

ISACA CISM Review Manual, Information Security Governance - third-party risk management and continuous assurance ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 125

A security incident has been reported within an organization When should an information security manager contact the information owner?

A. After the incident has been mitigated

B. After the incident has been confirmed.

C. After the potential incident has been togged

D. After the incident has been contained

Answer: (SHOW ANSWER)

= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident

response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

NEW QUESTION: 126
After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?
A. Calculating cost of the incident
B. Conducting a postmortem assessment
C. Performing an impact analysis
D. Preserving the evidence
Answer: (SHOW ANSWER)
The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future. References = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

NEW QUESTION: 127
Which of the following is the BEST way to reduce the risk of security incidents from targeted email attacks?
A. Implement a data loss prevention (DLP) system
B. Disable all incoming cloud mail services
C. Conduct awareness training across the organization
D. Require acknowledgment of the acceptable use policy
Answer: (SHOW ANSWER)
Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks.

Therefore, conducting awareness training across the organization is the correct answer.
References:
https://almanac.upenn.edu/articles/one-step-ahead-dont-get-caught-by-targeted-email-attacks
https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html

NEW QUESTION: 128
An information security manager wants to upgrade an organization's workstations to a new operating system version. Which of the following would be MOST helpful to gain senior management support for the upgrade?
A. An assessment of the current operating system based on risk
B. A summary of performance improvements in the new operating system
C. The results of user surveys indicating issues with the current operating system
D. A list of the latest security features in the new operating system
Answer: (SHOW ANSWER)
An assessment of the current operating system based on risk (A) is most effective for gaining senior management support because CISM emphasizes risk-based decision-making at the executive level. Senior management is primarily concerned with exposure, potential impact, and alignment with risk appetite-not technical features or user convenience. Performance improvements (B), user surveys (C), and feature lists (D) provide supporting detail but do not clearly articulate business risk. A risk-based assessment demonstrates why the upgrade is necessary to reduce unacceptable risk.
References: ISACA CISM Review Manual (Governance-executive communication, risk-based justification); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 129
Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?
A. Report the noncompliance to senior management
B. Validate the noncompliance
C. Implement compensating controls to mitigate the noncompliance
D. Include the noncompliance in the risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following is the PRIMARY reason that an information security manager should restrict the use of generic administrator accounts in a multi-user environment?
Freecram.net
A. To ensure system audit trails are not bypassed
B. To prevent accountability issues

C. To ensure separation of duties is maintained
D. To prevent unauthorized user access
Answer: (SHOW ANSWER)

NEW QUESTION: 131
Which of the following is MOST critical when creating an incident response plan?
A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Documenting incident notification and escalation processes
D. Aligning with the risk assessment process
Answer: (SHOW ANSWER)
= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION: 132
Which of the following is the MOST effective way to influence organizational culture to align with security guidelines?
A. Adhere to regulatory requirements
B. Conduct security awareness
C. Document and distribute security procedures
D. Communicate and enforce security policies
Answer: (SHOW ANSWER)
Communicating and enforcing policies demonstrates leadership commitment and drives behavior across the organization, fostering a culture of security.
"Policies must be effectively communicated and enforced to influence culture and employee behavior."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Security Culture*

NEW QUESTION: 133
Which of the following is MOST effective for communicating forward-looking trends within security reporting?
A. Key control indicator (KCIs)
B. Key risk indicators (KRIs)
C. Key performance indicators (KPIs)
D. Key goal indicators (KGIs)

Answer: (SHOW ANSWER)

= Security reporting is the process of providing relevant and timely information on the status and performance of the information security program to the stakeholders. Security reporting should be aligned with the business objectives and risk appetite of the organization, and should provide meaningful insights and recommendations for decision making and improvement. Security reporting should also include forward- looking trends, which are projections or predictions of future events or conditions based on historical data, current situation, and external factors. Forward-looking trends can help the organization anticipate and prepare for potential risks and opportunities, and adjust their strategies and plans accordingly.

One of the most effective ways to communicate forward-looking trends within security reporting is to use key risk indicators (KRIs). KRIs are metrics that measure the level of exposure or likelihood of a risk event occurring, and provide early warning signals of potential changes in the risk profile. KRIs can help the organization monitor and manage the key risks that may affect the achievement of their objectives, and take proactive actions to mitigate or avoid them. KRIs can also help the organization identify emerging risks and trends, and evaluate the effectiveness of their risk treatment options. KRIs should be aligned with the risk appetite and tolerance of the organization, and should be regularly reviewed and updated to reflect the changing risk environment.

The other options are not the most effective ways to communicate forward-looking trends within security reporting. Key control indicators (KCIs) are metrics that measure the effectiveness and efficiency of the security controls implemented to reduce the impact or likelihood of a risk event. KCIs can help the organization assess and improve the performance of their security processes and activities, and ensure compliance with the security policies and standards. However, KCIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key performance indicators (KPIs) are metrics that measure the achievement of the security objectives and goals, and demonstrate the value and contribution of the information security program to the organization. KPIs can help the organization evaluate and communicate the results and outcomes of their security initiatives and projects, and align them with the business strategy and vision. However, KPIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key goal indicators (KGIs) are metrics that measure the progress and completion of the security goals and targets, and indicate the degree of success and satisfaction of the information security program. KGIs can help the organization track and report the status and milestones of their security plans and actions, and ensure alignment with the stakeholder expectations and requirements.

However, KGIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 77-78, 81-821; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 4: Information Security Program Resources, ISACA2

NEW QUESTION: 134
Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?
A. Availability of web application firewall logs.
B. Capability of online virtual machine analysis
C. Availability of current infrastructure documentation
D. Capability to take a snapshot of virtual machines
Answer: (SHOW ANSWER)
A snapshot is a point-in-time copy of the state of a virtual machine (VM) that can be used to restore the VM to a previous state in case of a security incident or a disaster. A snapshot can capture the VM's disk, memory, and device configuration, allowing for a quick and easy recovery of the VM's data and functionality.
Snapshots can also be used to create backups, clones, or replicas of VMs for testing, analysis, or migration purposes. Snapshots are a common service offering in Infrastructure as a Service (IaaS) models, where customers can provision and manage VMs on demand from a cloud service provider (CSP). A CSP that offers the capability to take snapshots of VMs can assist customers when recovering from a security incident by providing them with the following benefits12:
Faster recovery time: Snapshots can reduce the downtime and data loss caused by a security incident by allowing customers to quickly revert their VMs to a known good state. Snapshots can also help customers avoid the need to reinstall or reconfigure their VMs after an incident, saving time and resources.
Easier incident analysis: Snapshots can enable customers to perform online or offline analysis of their VMs after an incident, without affecting the production environment. Customers can use snapshots to examine the VM's disk, memory, and logs for evidence of compromise, root cause analysis, or forensic investigation.
Customers can also use snapshots to test and validate their incident response plans or remediation actions before applying them to the production VMs.
Enhanced security posture: Snapshots can improve the security posture of customers by enabling them to implement best practices such as backup and restore, disaster recovery, and business continuity. Snapshots can help customers protect their VMs from accidental or malicious deletion, corruption, or modification, as well as from environmental or technical disruptions. Snapshots can also help customers comply with regulatory or contractual requirements for data retention, availability, or integrity. References = What is Disaster Recovery as a Service? | CSA - Cloud Security Alliance, What Is Cloud Incident Response (IR)?
CrowdStrike

NEW QUESTION: 135
An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?
A. Establishing the authority to remote wipe

B. Developing security awareness training
C. Requiring the backup of the organization's data by the user
D. Monitoring how often the smartphone is used
Answer: (SHOW ANSWER)
The best security control for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones is establishing the authority to remote wipe. Remote wipe is a feature that allows an authorized administrator or user to remotely erase the data on a device in case of loss, theft, or compromise1. Remote wipe can help prevent unauthorized access or disclosure of the organization's information on employee-owned smartphones, as well as protect the privacy of the employee's personal data.
Remote wipe can be implemented through various methods, such as mobile device management (MDM) software, native device features, or third-party applications2. However, remote wipe requires the consent and cooperation of the employee, as well as a clear policy that defines the conditions and procedures for its use.
The other options are not the best security controls for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones. Developing security awareness training is an important measure to educate employees about the security risks and responsibilities associated with using their own smartphones for work purposes, but it does not provide a technical or physical protection for the data on the devices3. Requiring the backup of the organization's data by the user is a good practice to ensure data availability and recovery in case of device failure or loss, but it does not prevent unauthorized access or disclosure of the data on the devices4. Monitoring how often the smartphone is used is a possible way to detect abnormal or suspicious activities on the devices, but it does not prevent or mitigate the impact of a data breach on the devices. References: 4: Mobile Device Backup - NIST 3: Security Awareness Training - NIST
1: Remote Wipe - Lifewire 2: How Businesses with a BYOD Policy Can Secure Employee Devices - IBM :
Mobile Device Security Policy - SANS

NEW QUESTION: 136
Which of the following is the MOST effective way to demonstrate alignment of information security strategy with business objectives?
A. Balanced scorecard
B. Risk matrix
C. Benchmarking
D. Heat map
Answer: (SHOW ANSWER)
The most effective way to demonstrate alignment of information security strategy with business objectives is to use a balanced scorecard. A balanced scorecard is a strategic management tool that translates the vision and mission of an organization into a set of performance indicators that measure its progress towards its goals. A balanced scorecard typically includes four perspectives:

financial, customer, internal process, and learning and growth. Each perspective has a set of objectives, measures, targets, and initiatives that are aligned with the organization's strategy. A balanced scorecard helps to communicate, monitor, and evaluate the performance of the organization and its information security program in relation to its business objectives. A balanced scorecard also helps to identify and prioritize improvement opportunities, as well as to align the activities and resources of the organization with its strategy12.
The other options are not the most effective ways to demonstrate alignment of information security strategy with business objectives. A risk matrix is a tool that displays the likelihood and impact of various risks on a two-dimensional grid. A risk matrix helps to assess and prioritize risks, as well as to determine the appropriate risk response strategies. However, a risk matrix does not show how the information security strategy supports the business objectives, nor does it measure the performance or the value of the information security program3. Benchmarking is a process of comparing the performance, practices, or processes of an organization with those of other organizations or industry standards. Benchmarking helps to identify best practices, gaps, and areas for improvement, as well as to set realistic and achievable goals. However, benchmarking does not show how the information security strategy aligns with the business objectives, nor does it reflect the unique characteristics and needs of the organization4. A heat map is a graphical representation of data using colors to indicate the intensity or frequency of a variable. A heat map can be used to visualize the distribution, concentration, or variation of risks, controls, or incidents across different dimensions, such as business units, processes, or assets. A heat map helps to highlight the areas of high risk or low control effectiveness, as well as to facilitate decision making and resource allocation. However, a heat map does not show how the information security strategy contributes to the business objectives, nor does it measure the outcomes or the benefits of the information security program5. References = CISM Review Manual, 16th Edition | Print | English 2, Chapter 1: Information Security Governance, pages 28-29, 31-32, 34-35.
Balanced Scorecard - Wikipedia 1
Risk Matrix - Wikipedia 3
Benchmarking - Wikipedia 4
Heat map - Wikipedia 5

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137

The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do NEXT?

A. Review the risk monitoring plan.

B. Formally document the decision.

C. Review the regulations.

D. Advise the risk management team.

Answer: (SHOW ANSWER)

Since the identified risks are subject to regulatory requirements, and cannot simply be accepted without oversight, the information security manager should escalate the issue to the risk management team or higher authority to ensure proper governance.

"When risk acceptance contradicts regulatory requirements, it must be escalated to senior management or the risk function for resolution."

- CISM Review Manual 15th Edition, Chapter 1: Governance Responsibilities, Section: Risk Governance and Oversight*

NEW QUESTION: 138

Which of the following BEST determines an information asset's classification?

A. Value of the information asset in the marketplace

B. Criticality to a business process

C. Risk assessment from the data owner

D. Cost of producing the information asset

Answer: (SHOW ANSWER)

According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.

References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

NEW QUESTION: 139

An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

A. a control self-assessment (CSA) process.

B. automated reporting to stakeholders.

C. a monitoring process for the security policy.

D. metrics for each milestone.

Answer: (SHOW ANSWER)

= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress,

performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.

The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self- assessment (CSA) process is a technique to involve the staff in assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.

CISM domain 1: Information security governance [Updated 2022], Infosec, 1.

Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

NEW QUESTION: 140

Which of the following is the BEST indicator of an organization's information security status?

A. Intrusion detection log analysis

B. Controls audit

C. Threat analysis

D. Penetration test

Answer: (SHOW ANSWER)

A controls audit is the best indicator of an organization's information security status, as it provides an independent and objective assessment of the design, implementation, and effectiveness of the information security controls. A controls audit can also identify the strengths and weaknesses of the information security program, as well as the compliance with the policies, standards, and regulations. A controls audit can cover various aspects of information security, such as governance, risk management, incident management, business continuity, and technical security. A controls audit can be conducted by internal or external auditors, depending on the scope, purpose, and frequency of the audit.
The other options are not as good as a controls audit, as they do not provide a comprehensive and holistic view of the information security status. Intrusion detection log analysis is a technique to monitor and analyze the network or system activities for signs of unauthorized or malicious access or attacks. It can help to detect and respond to security incidents, but it does not measure the overall performance or maturity of the information security program. Threat analysis is a process to identify and evaluate the potential sources, methods, and impacts of threats to the information assets. It can help to prioritize and mitigate the risks, but it does not verify the adequacy or functionality of the information security controls. Penetration test is a simulated attack on the network or system to evaluate the vulnerability and exploitability of the information security defenses. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1012.

NEW QUESTION: 141
An information security manager has confirmed the organization's cloud provider has unintentionally published some of the organization's business data. Which of the following should be done NEXT?
A. Invoke the incident response plan.
B. Initiate the organization's data loss prevention (DLP) processes.
C. Review the cloud provider's service level agreement (SLA).
D. Identify users associated with the exposed data.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Which of the following should an information security manager do FIRST after identifying suspicious activity on a PC that is not in the organization's IT asset inventory?
A. Isolate the PC from the network
B. Perform a vulnerability scan
C. Determine why the PC is not included in the inventory
D. Reinforce information security training
Answer: C (LEAVE A REPLY)

The first thing an information security manager should do after identifying suspicious activity on a PC that is not in the organization's IT asset inventory is to determine why the PC is not included in the inventory. This will help to identify the source and scope of the threat, as well as the potential impact and risk to the organization. The IT asset inventory is a list of all the hardware, software, data, and other resources that are owned, controlled, or used by an organization. It helps to establish accountability, visibility, and control over the IT assets, as well as to support security policies and procedures.
If a PC is not included in the inventory, it may indicate that it has been compromised by an unauthorized user or entity, or that it has been moved or transferred without proper authorization. It may also indicate that there are gaps or errors in the inventory management process, such as missing records, duplicate entries, outdated information, or inaccurate classification. These issues can pose significant challenges for information security management, such as:
* Lack of visibility into the IT environment and assets
* Difficulty in detecting and responding to incidents
* Increased risk of data breaches and cyberattacks
* Non-compliance with regulatory requirements and standards
* Reduced trust and confidence among stakeholders
Therefore, an information security manager should take immediate steps to investigate why the PC is not included in the inventory and take appropriate actions to remediate the situation.
References = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Inventory Management1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 143
When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?
A. Recommendations from senior management
B. Vulnerability assessment results
C. Business impact analysis (BIA) results
D. The business continuity plan (BCP)
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?
A. Perform a risk assessment.
B. Reduce security hardening settings.
C. Inform business management of the risk.
D. Document a security exception.
Answer: (SHOW ANSWER)

Security hardening is the process of applying security configuration settings to systems and software to reduce their attack surface and improve their resistance to threats1. Security hardening settings are based on industry standards and best practices, such as the CIS Benchmarks2, which provide recommended security configurations for various software applications, operating systems, and network devices. However, security hardening settings may not always be compatible with the business requirements and objectives of an organization, and may negatively impact the functionality, performance, or usability of the systems and software3. Therefore, before applying any security hardening settings, an information security manager should perform a risk assessment to evaluate the potential benefits and drawbacks of the settings, and to identify and prioritize the risks associated with them. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses.
A risk assessment helps the information security manager to balance the security and business needs of the organization, and to communicate the risk level and impact to the relevant stakeholders. A risk assessment should be performed first, before taking any other actions, such as reducing security hardening settings, informing business management of the risk, or documenting a security exception, because it provides the necessary information and justification for making informed and rational decisions. References = 1: Basics of the CIS Hardening Guidelines | RSI Security 2: CIS Baseline Hardening and Security Configuration Guide | CalCom 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 145 : CISM Review Manual 15th Edition, page 146 : CISM Review Manual 15th Edition, page 147

NEW QUESTION: 145
Which of the following roles is accountable for the protection of data?
A. CISO
B. Data custodian
C. Data owner
D. Data administrator
Answer: C (LEAVE A REPLY)
Under CISM governance principles, the data owner is accountable for the protection of data. Accountability includes decisions regarding data classification, access authorization, acceptable use, retention, and risk acceptance. While the CISO (A) provides oversight and guidance, they are not accountable for individual data assets. Data custodians (B) and administrators (D) are responsible for implementing and operating controls but do not own the business risk associated with the data. CISM clearly distinguishes accountability (business) from responsibility (operational/technical). Assigning accountability to the data owner ensures that protection requirements align with business value, regulatory obligations, and risk appetite.
References: ISACA CISM Review Manual (Governance-roles and responsibilities, information asset ownership); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 146
An organization's quality process can BEST support security management by providing:
A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.
Answer: (SHOW ANSWER)
= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct security defects, measure security performance and effectiveness, and improve security practices and procedures. References = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

NEW QUESTION: 147
An organization has identified an active cyberattack on its internal network. Which of the following considerations is MOST important to the success of the incident response?
A. The data loss prevention tool is functioning properly
B. Contact details for forensics support are readily available
C. The recovery time objective can be met
D. Communication to stakeholders is conducted through a separate channel
Answer: (SHOW ANSWER)
The correct answer is D because during an active cyberattack on the internal network, normal communication channels may be compromised, monitored, disrupted, or manipulated by the attacker. Conducting stakeholder communication through a separate and trusted channel helps preserve confidentiality, integrity, and coordination during response. Effective incident response depends on secure communication among the response team, management, legal, technical teams, external support, and other stakeholders. A functioning data loss prevention tool may help detect or prevent data exfiltration, but it is only one technical control and may not be central to response coordination. Forensics contact details are useful, but they do not guarantee secure coordination during an active attack. Meeting the recovery time objective is important during recovery, but the immediate success of incident response depends on containment, coordination, and trusted communication. CISM incident management emphasizes communication planning, escalation, stakeholder coordination, and reducing business impact. Therefore, using a separate

communication channel is the most important consideration during an active internal network attack.
Reference: CISM Information Security Incident Management; incident communication, secure channels, active attack response, stakeholder coordination, and containment principles.

NEW QUESTION: 148
To effectively manage an organization ' s information security risk, it is MOST important to:
A. assign risk management responsibility to an experienced consultant.
B. periodically identify and correct new systems vulnerabilities.
C. establish and communicate risk tolerance.
D. benchmark risk scenarios against peer organizations.
Answer: (SHOW ANSWER)
To effectively manage an organization's information security risk, it is most important to establish and communicate risk tolerance, which is the level of risk that the organization is willing to accept or bear. By establishing and communicating risk tolerance, the organization can align its risk management strategy and objectives with its business goals and values, and ensure that the risk management activities and decisions are consistent and appropriate across the organization.
References: The CISM Review Manual 2023 defines risk tolerance as "the acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives" and states that
"the information security manager should assist the enterprise in establishing and communicating its risk tolerance, and ensure that the risk management process is aligned with the enterprise's risk tolerance" (p. 94).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Establish and communicate risk tolerance is the correct answer because it is the most important factor to effectively manage an organization's information security risk, as it helps to define the scope, direction, and priorities of the risk management process, and to ensure that the risk management activities and decisions are consistent and appropriate across the organization" (p. 29). Additionally, the article Risk Tolerance: The Forgotten Factor from the ISACA Journal 2019 states that "risk tolerance is the key factor that influences the risk management process and outcomes" and that "risk tolerance should be established and communicated by the organization's senior management and board of directors, and should reflect the organization's strategy, culture, and governance" (p. 1)1

NEW QUESTION: 149
Which of the following BEST enables the effectiveness of an information security training program for new employees?
A. The training is specific to new employees' job functions.
B. New employees are required to acknowledge the information security policy.
C. New employees must complete a security assessment after training.
D. Information security training precedes all other onboarding training.

Answer: (SHOW ANSWER)

The correct answer is A because information security training is most effective when it is relevant to the employee's job function. Role-based training helps new employees understand the specific risks, responsibilities, systems, data types, and expected behaviors related to their work. For example, developers need secure coding guidance, finance staff need fraud and payment security awareness, and human resources staff need privacy and personnel data protection training. Requiring acknowledgement of the information security policy is useful for accountability, but it does not ensure that employees understand how security applies to their roles. A post-training assessment can help measure understanding, but it does not by itself make the training effective. Conducting security training before all other onboarding may show priority, but timing is less important than relevance and applicability. In CISM, effective awareness and training programs should be targeted, risk-based, and aligned with users' responsibilities. Therefore, job-function-specific training best enables effectiveness.

Reference: CISM Information Security Program Development and Management; security awareness, role- based training, employee onboarding, and user responsibility principles.

NEW QUESTION: 150

Which of the following BEST indicates misalignment of security policies with business objectives?

A. Lack of adequate funding for the security program

B. Low completion rate of employee awareness training

C. A large number of user noncompliance incidents

D. A large number of long-term policy exceptions

Answer: (SHOW ANSWER)

NEW QUESTION: 151

Which of the following is the BEST way to ensure the business continuity plan (BCP) is current?

A. Manage business process changes.

B. Update business impact analyses (BIAs) on a regular basis.

C. Conduct periodic testing.

D. Review and update emergency contact lists.

Answer: C (LEAVE A REPLY)

Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.

References: The CISM Review Manual 2023 states that "testing is a critical component of the BCP process" and that "testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations" (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Conducting periodic testing is the correct answer because it is the best way to ensure

the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update" (p. 98). Additionally, the article Business Continuity Planning: Testing an Organization's Plan from the ISACA Journal 2019 states that "testing is essential to ensure that the BCP is current and effective" and that "testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks" (p. 1)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 152
An information security manager finds a legacy application has no defined data owner. Of the following, who would be MOST helpful in identifying the appropriate data owner?
A. The individual who has the most privileges within the application
B. The individual who manages the process supported by the application
C. The individual responsible for providing support for the application
D. The individual who manages users of the application
Answer: B (LEAVE A REPLY)
In CISM governance, data ownership is a business accountability, not an IT/technical one. The most helpful person to identify the correct data owner is the individual who manages the business process supported by the application (B), because they are closest to the business purpose, outcomes, and decision-making authority tied to that information. Data owners are typically accountable for data classification, access authorization, acceptable use, retention requirements, and protection needs aligned with business and regulatory obligations.
By contrast, the person with the most privileges (A) is often an admin and may only reflect technical access, not accountability. Application support (C) manages operational upkeep, and user management (D) may administer accounts but does not define business responsibility for the information. Assigning the right owner is critical to enable proper governance controls such as access approvals, risk acceptance, and compliance decisions-especially for legacy systems where responsibilities can drift over time.
References: ISACA CISM Review Manual (Governance-roles and responsibilities, information asset ownership, accountability model); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 153

Which of the following is the BEST way to evaluate the effectiveness of physical and environmental security controls implemented for fire-related disasters?
A. Conduct evacuation exercises
B. Review the disaster recovery plan (DRP)
C. Conduct awareness sessions
D. Review emergency management team procedures
Answer: (SHOW ANSWER)
Evacuation drills provide real-time validation of physical security measures, staff preparedness, and response time during fire-related scenarios. They test both people and systems.
"Simulated exercises are the most effective method to evaluate real-world preparedness and the adequacy of response procedures."
- CISM Review Manual 15th Edition, Chapter 3: Security Controls Testing* Paper reviews and awareness are useful, but only exercises reveal actual gaps in preparedness.

NEW QUESTION: 154
An organization is in the process of selecting a third party to process customer information. Which of the following provides the BEST evidence that the third party's controls will operate as required?
A. Results of incident response tests
B. An independent assessment
C. An external vulnerability assessment
D. An information security questionnaire
Answer: (SHOW ANSWER)
The correct answer is B because an independent assessment provides objective evidence regarding the design and operating effectiveness of a third party's controls. When a vendor will process customer information, the organization must obtain assurance that the vendor can protect confidentiality, integrity, availability, privacy, and regulatory compliance requirements. Independent assessments, such as third-party audit reports or assurance reviews, are stronger than self-reported information because they are performed by an objective party. Incident response test results may show one aspect of readiness, but they do not provide broad evidence that all required controls operate effectively. An external vulnerability assessment is useful for identifying technical weaknesses, but it is limited in scope. A questionnaire can help gather information during due diligence, but it relies heavily on vendor representations. CISM emphasizes third-party risk management, due diligence, contractual assurance, and ongoing monitoring. Therefore, an independent assessment is the best evidence that the third party's controls will operate as required.
Reference: CISM Information Risk Management; third-party risk management, vendor assurance, due diligence, and control assessment principles.

NEW QUESTION: 155

A department has reported that a security control is no longer effective. Which of the following is the information security manager's BEST course of action?

A. Replace the control

B. Check for defense in depth

C. Assess the control state

D. Report the failure to management

Answer: (SHOW ANSWER)

The best first step is to assess the control state to determine why it is ineffective and whether adjustments, replacements, or compensating controls are needed.

"Regularly assess the effectiveness of security controls to ensure they are providing the intended level of protection."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Control Monitoring and Assessment* ISACA practice questions stress that assessing the control state comes before taking further action.

NEW QUESTION: 156

In which cloud model does the cloud service buyer assume the MOST security responsibility?

A. Disaster Recovery as a Service (DRaaS)

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) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment.

In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page

140-1411

NEW QUESTION: 157
Of the following, who is MOST appropriate to own the risk associated with the failure of a privileged access control?
A. Data owner
B. Business owner
C. Information security manager
D. Compliance manager
Answer: (SHOW ANSWER)
The business owner is the most appropriate person to own the risk associated with the failure of a privileged access control because they are ultimately responsible for the protection and use of the information in their business unit1. The data owner is responsible for determining the access rights for specific data sets, but not for the access control mechanisms2. The information security manager is responsible for implementing and enforcing the security policies and standards, but not for owning the risk3. The compliance manager is responsible for ensuring that the organization meets the regulatory requirements, but not for owning the risk3.
References: 1 https://www.cyberark.com/resources/blog/how-do-you-prioritize-risk-for-privileged-access- management 3 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for- privileged-access-management 2 https://security.stackexchange.com/questions/218049/what-is-the-difference- between-data-owner-data-custodian-and-system-owner

NEW QUESTION: 158
After detecting an advanced persistent threat, which of the following should be the information security manager's FIRST step?
A. Notify affected stakeholders
B. Conduct a vulnerability analysis
C. Perform a root cause analysis
D. Remove the threat
Answer: (SHOW ANSWER)
The correct answer is D because once an advanced persistent threat has been detected, the immediate priority is to stop or limit ongoing harm to the organization. In practical incident response, this normally involves containment and eradication activities, such as isolating compromised systems, disabling attacker access, blocking malicious communication, and removing the threat from the environment. The option "remove the threat" is the closest available answer to immediate containment and eradication. Notifying affected stakeholders is important, but premature or poorly timed communication before controlling the threat may increase confusion or exposure. Vulnerability analysis and root cause analysis are valuable follow-up activities, but they are not the first priority while an active threat may still be operating. CISM incident management emphasizes minimizing business impact, preserving essential services, and

executing predefined response procedures. For an APT, the organization must act quickly and carefully to limit attacker persistence, prevent further compromise, and protect critical assets. Therefore, removing the threat is the best first action among the choices given.
Reference: CISM Information Security Incident Management; incident containment, eradication, threat response, and impact reduction principles.

NEW QUESTION: 159
Which of the following processes is MOST important for the success of a business continuity plan?
A. Including the board and senior management in plan reviews
B. Maintaining copies of the plan at the primary and recovery sites
C. Scheduling periodic internal and external audits
D. Involving all stakeholders in testing and training
Answer: (SHOW ANSWER)
The correct answer is D because a business continuity plan is successful only when relevant stakeholders understand their roles and can execute the plan effectively during a disruption. Testing and training involving all stakeholders validate assumptions, communication paths, responsibilities, dependencies, recovery procedures, supplier coordination, and escalation processes. Board and senior management involvement in plan reviews is important for governance and support, but operational success depends on the people who must perform the plan. Maintaining copies at primary and recovery sites is useful for accessibility, but having the plan available does not ensure it can be executed. Periodic audits can identify gaps and provide assurance, but audits do not substitute for practical training and testing. CISM incident management and continuity principles emphasize preparedness, exercises, communication, stakeholder participation, and continuous improvement. Because business continuity requires coordinated action across business units, IT, suppliers, management, and support functions, involving all stakeholders in testing and training is the most important process for success.
Reference: CISM Information Security Incident Management; business continuity planning, stakeholder training, BCP testing, and preparedness.

NEW QUESTION: 160
Which of the following BEST encourages staff to report issues related to information security?
A. Tabletop exercises are performed on a regular basis
B. Incentives are offered for security skills training
C. The leaders set a positive security culture
D. Formal incident response processes are in place
Answer: (SHOW ANSWER)
The correct answer is C because staff are more likely to report information security issues when leadership establishes a positive security culture. A positive culture encourages openness, trust, accountability, and timely reporting without fear of unfair blame. In CISM governance, information security is not only a technical function; it depends heavily on behavior, communication,

leadership support, and organizational values. Tabletop exercises are useful for testing incident response readiness, but they do not necessarily encourage everyday reporting by all staff. Incentives for security skills training may improve participation in learning activities, but they do not directly create a reporting culture. Formal incident response processes are important because they define how incidents are handled, but processes alone may not motivate employees to report concerns if the culture is negative or punitive. Leadership behavior is critical because employees follow the tone set by management. Therefore, leaders setting a positive security culture is the best way to encourage staff to report information security issues.
Reference: CISM Information Security Governance; security culture, leadership commitment, awareness, reporting, and accountability principles.

NEW QUESTION: 161
A business continuity plan (BCP) should contain:
A. Hardware and software inventories
B. Data restoration procedures
C. Information about eradication activities
D. Criteria for activation
Answer: (SHOW ANSWER)
Criteria for activation are essential to ensure that the BCP is triggered appropriately in response to a disruption.
"The BCP should include clearly defined activation criteria to ensure that plans are invoked when necessary."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Planning* ISACA's practice questions confirm that criteria for activation are core to a BCP's effectiveness.

NEW QUESTION: 162
Which of the following BEST ensures information security governance is aligned with corporate governance?
A. A security steering committee including IT representation
B. A consistent risk management approach
C. An information security risk register
D. Integration of security reporting into corporate reporting
Answer: (SHOW ANSWER)
The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with

corporate governance by themselves. References = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

NEW QUESTION: 163
Which of the following is the BEST way to determine if an information security profile is aligned with business requirements?
A. Review the key performance indicator (KPI) dashboard
B. Review security-related key risk indicators (KRIs)
C. Review control self-assessment (CSA) results
D. Review periodic security audits
Answer: (SHOW ANSWER)
Security-related KRIs are metrics that measure the effectiveness of the information security profile in achieving the business objectives and managing the risks. Reviewing security-related KRIs can help to determine if the information security profile is aligned with business requirements, as they reflect the security performance and outcomes that are relevant for the business. Reviewing other options, such as KPIs, CSAs, or audits, may provide some insights into the security status, but they are not the best way to assess the alignment with business requirements, as they may not capture the business context and goals adequately.
References:
* https://www.nist.gov/cyberframework/examples-framework-profiles
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/accountability-for-information- security-roles-and-responsibilities-part-1
* https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea- top-down-approach

NEW QUESTION: 164
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders
Answer: (SHOW ANSWER)
= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them.
By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned

with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION: 165
An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?
A. Focus the review on the infrastructure with the highest risk
B. Review controls listed in the vendor contract
C. Determine whether the vendor follows the selected security framework rules
D. Review the vendor's security policy
Answer: (SHOW ANSWER)
Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization's data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor's security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices.
Therefore, reviewing controls listed in the vendor contract is the correct answer.
References:
https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/
https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf
https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

NEW QUESTION: 166
Which of the following is MOST important to have in place for an organization's information security program to be effective?
A. Documented information security processes
B. A comprehensive IT strategy
C. Senior management support
D. Defined and allocated budget
Answer: (SHOW ANSWER)
Senior management support is the most important factor to have in place for an organization's information security program to be effective because it helps to establish the vision, direction, and goals of the program, as well as to allocate the necessary resources and authority to implement and maintain it. Senior management support also helps to foster a security culture within the organization, where security is seen as a shared responsibility and a business enabler. Senior

management support also helps to ensure compliance with internal and external security policies and standards, as well as to communicate the value and impact of security to stakeholders. Therefore, senior management support is the correct answer.
References:
* https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for- security-governance-part-1
* https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf
* https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 167
Embedding security responsibilities into job descriptions is important PRIMARILY because it:
A. supports access management.
B. simplifies development of the security awareness program.
C. aligns security to the human resources (HR) function.
D. strengthens employee accountability.
Answer: (SHOW ANSWER)
Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

NEW QUESTION: 168
Which of the following will BEST enable an organization to meet incident response requirements when outsourcing its incident response function?
A. Including response times in service level agreements (SLAs)
B. Contracting with a well-known incident response provider

C. Requiring comprehensive response applications and tools
D. Including a right-to-audit clause in service level agreements (SLAs)
Answer: (SHOW ANSWER)

NEW QUESTION: 169
To ensure the information security of outsourced IT services, which of the following is the MOST critical due diligence activity?
A. Review samples of service level reports from the service provider.
B. Assess the level of security awareness of the service provider.
C. Review a recent independent audit report of the service provider.
D. Request the service provider comply with information security policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?
Freecram.net
A. Business continuity coordinator
B. Information security manager
C. Business process owner
D. Senior management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
Which of the following BEST determines the allocation of resources during a security incident response?
A. Senior management commitment
B. A business continuity plan (BCP)
C. An established escalation process
D. Defined levels of severity
Answer: (SHOW ANSWER)
= The allocation of resources during a security incident response depends on the defined levels of severity, which indicate the potential impact and urgency of the incident. The levels of severity help prioritize the response activities and assign the appropriate roles and responsibilities. Senior management commitment, a business continuity plan (BCP), and an established escalation process are important factors for an effective incident response, but they do not directly determine the allocation of resources. References = CISM Review Manual, 16th Edition, page 3011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462 Learn more:
1. isaca.org2. amazon.com3. gov.uk
Defined levels of severity is the best determinant of the allocation of resources during a security incident response. Having defined levels of severity allows organizations to plan for and allocate resources for each level of incident, depending on the severity of the incident. This ensures that

the right resources are allocated in a timely manner and that incidents are addressed appropriately.

NEW QUESTION: 172
Which of the following is the BEST way to compete for funding for an information security program in an organization with limited resources?
A. Demonstrate the effectiveness of business continuity plans (BCPs).
B. Report key performance indicator (KPI) trends.
C. Demonstrate that the program enables business activities.
D. Provide evidence of increased security events at peer organizations.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
The goal of securing funding for an information security program often requires aligning the program with business goals and demonstrating its value to the organization. Here's an analysis of each option:
A). Demonstrate the effectiveness of business continuity plans (BCPs): While important, this focuses on continuity rather than the overall value of the information security program to business objectives. This is not the strongest method to justify funding.
B). Report key performance indicator (KPI) trends: KPI trends are useful for tracking performance but may not directly demonstrate how the program supports business activities or adds value.
C). Demonstrate that the program enables business activities: This is the BEST option because it ties the information security program directly to business operations. When security is seen as an enabler (e.g., reducing risks in critical areas like customer data protection), stakeholders are more likely to allocate resources.
D). Provide evidence of increased security events at peer organizations: This may indicate a general threat landscape but does not provide concrete evidence of the program's value or relevance to the organization's specific goals.
Reference: CISM Job Practice Area 1 (Information Security Governance) emphasizes aligning information security strategies with organizational objectives to gain stakeholder support.

NEW QUESTION: 173
From an information security perspective, legal issues associated with a transborder flow of technology- related items are MOST often
A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.
Answer: (SHOW ANSWER)
Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to

different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. References: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on- transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

NEW QUESTION: 174
Which of the following is the MOST effective way to determine the alignment of an information security program with the business strategy?
A. Evaluate the results of business continuity testing.
B. Review key performance indicators (KPIs).
C. Evaluate the business impact of incidents.
D. Engage business process owners.
Answer: (SHOW ANSWER)
The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.
Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

NEW QUESTION: 175
An organization would like to invest in a new emerging technology. Which of the following is MOST important for the information security manager to consider when evaluating its impact?

A. Industry peer reviews of the technology
B. Vulnerabilities in the technology
C. Secure configuration
D. Systems compatibility
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Which of the following BEST enables an organization to transform its culture to support information security?
A. Periodic compliance audits
B. Strong management support
C. Robust technical security controls
D. Incentives for security incident reporting
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), page 5, information security culture is the set of values, attitudes, and behaviors that shape how an organization and its employees view and practice information security. Transforming the information security culture requires a change management process that involves the following steps: creating a sense of urgency, forming a powerful coalition, developing a vision and strategy, communicating the vision, empowering broad-based action, generating short-term wins, consolidating gains and producing more change, and anchoring new approaches in the culture1. Among the four options, strong management support is the best enabler for transforming the information security culture, as it can provide the necessary leadership, resources, sponsorship, and alignment for the change management process. Periodic compliance audits, robust technical security controls, and incentives for security incident reporting are important elements of information security, but they are not sufficient to change the culture without strong management support. References = 1: CISM Review Manual (Digital Version), page 5

NEW QUESTION: 177
An organization is transitioning to a Zero Trust architecture. Which of the following is the information security manager's BEST approach for communicating the implications of this transition to the board of directors?
A. Present a diagram of core Zero Trust logical components to help visualize the architectural changes
B. Summarize the training plan and end user feedback in an internal portal and send the link to the board
C. Prepare a report on the Zero Trust implementation that includes a status dashboard and timeline
D. Provide an outline of the business impact in terms of risk reduction and changes in user experience
Answer: (SHOW ANSWER)

Senior leadership needs to understand how Zero Trust supports risk reduction and business needs.
Communicating the impact on risk reduction and user experience aligns security initiatives with business goals.
"Communicating how security initiatives support business objectives and risk reduction is critical for gaining senior management support."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment*

NEW QUESTION: 178
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?
A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems
Answer: (SHOW ANSWER)
The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.
The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non- compliance. However, SLAs do not necessarily address the specific procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties. Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems. However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that

could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management. References = 1, 2, 3, 4, 5 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident-management- part-1 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident- management-part-1

NEW QUESTION: 179

The manager of a key project has bypassed the standard contractor onboarding process to acquire additional resources for delivering the project on time. Contracts were executed offline, and contractors were provided organizational access without going through the standard due diligence process. Which of the following should be the PRIMARY concern?

A. The contractors may inappropriately outsource the business functions to fourth-party suppliers

B. There are insufficient contractual requirements in place to govern third-party arrangements

C. The project may be delayed further if the incident is reported

D. The contractors may not operate in line with industry benchmarks

Answer: B (LEAVE A REPLY)

The correct answer is B because bypassing the standard onboarding and due diligence process creates a major third-party risk, especially where contracts were executed offline and access was granted without proper review. The primary concern is that the organization may lack sufficient contractual security, privacy, compliance, audit, service, incident notification, confidentiality, and termination requirements to govern the contractor relationship. Fourth-party outsourcing is possible, but it is only one risk that should normally be controlled through contract terms and due diligence. Further project delay is a business concern, but it should not override security and risk management requirements. Industry benchmarks may be useful, but they are not the main issue. CISM risk management principles require that third-party relationships be governed through due diligence, risk assessment, clearly defined responsibilities, access controls, and enforceable contractual obligations. Granting organizational access without proper contractual and risk controls can expose sensitive information, systems, and business processes to unacceptable risk. Reference: CISM Information Risk Management; third-party risk management, contractor onboarding, due diligence, access governance, and contractual control principles.

NEW QUESTION: 180

Which of the following should be the MOST important consideration of business continuity management?

Freecram.net

A. Ensuring human safety

B. Identifying critical business processes

C. Ensuring the reliability of backup data

D. Securing critical information assets

Answer: (SHOW ANSWER)

= Business continuity management (BCM) is the process of planning and implementing measures to ensure the continuity of critical business processes in the event of a disruption. The most

important consideration of BCM is ensuring human safety, as this is the primary responsibility of any organization and the basis of ethical conduct. Human safety includes protecting the health and well-being of employees, customers, suppliers, and other stakeholders who may be affected by a disruption. Identifying critical business processes, ensuring the reliability of backup data, and securing critical information assets are also important aspects of BCM, but they are secondary to human safety. References = CISM Review Manual, 16th Edition, ISACA,
2020, p. 2111; CISM Online Review Course, Domain 4: Information Security Incident Management, Module
4: Business Continuity and Disaster Recovery, ISACA2

NEW QUESTION: 181
Which of the following is MOST appropriate to communicate to senior management regarding information risk?
A. Emerging security technologies
B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress
Answer: (SHOW ANSWER)
Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2:
Information Risk Management (IRM) [2022 update]

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here:
https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 182

An information security manager has completed a risk assessment for a business information system. Of the following, who is BEST positioned to decide on the implementation of mitigating controls?

A. System administrator

B. System owner

C. Chief information officer

D. Risk manager

Answer: (SHOW ANSWER)

The correct answer is B because the system owner is best positioned to decide on the implementation of mitigating controls for a business information system. The system owner is accountable for the system's business purpose, data, operational impact, and associated risk. After a risk assessment identifies threats, vulnerabilities, likelihood, impact, and recommended controls, the system owner must decide which risk treatment actions are appropriate based on business needs, risk appetite, cost, and operational requirements. A system administrator may implement technical controls, but does not normally own the business risk. The chief information officer may provide technology oversight, but may not be the accountable owner of the specific business system. The risk manager facilitates the risk management process and provides guidance, but risk treatment decisions belong to the risk or system owner. In CISM, business ownership and accountability are central principles. Information security managers advise and recommend, but accountable business or system owners decide on mitigation.

Reference: CISM Information Risk Management; risk ownership, system ownership, risk treatment, and control implementation accountability principles.

NEW QUESTION: 183

An online trading company discovers that a network attack has penetrated the firewall. What should be the information security manager's FIRST response?

A. Evaluate the impact to the business.

B. Examine firewall logs to identify the attacker.

C. Implement mitigating controls.

D. Notify the regulatory agency of the incident.

Answer: (SHOW ANSWER)

NEW QUESTION: 184

Which of the following is the PRIMARY reason for conducting an incident response tabletop exercise?

A. To define incident response resource needs

B. To mature the organization's information security program

C. To prepare the incident response team for a real-world event

D. To provide the status of incident response preparedness to leadership

Answer: C (LEAVE A REPLY)

The primary purpose of a tabletop exercise is to prepare the incident response team for a real-world event (C).
Tabletop exercises allow participants to walk through scenarios, clarify roles and responsibilities, validate decision-making, and identify gaps in procedures-without the disruption of a live incident. While outcomes may inform resource needs (A), program maturity (B), or leadership reporting (D), these are secondary benefits. CISM emphasizes regular testing of incident response capabilities to ensure teams can respond quickly, consistently, and effectively under pressure.
References: ISACA CISM Review Manual (Incident management-testing, exercises, and readiness); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 185
A new risk has been identified in a high availability system. The BEST course of action is to:
A. Perform a cost-benefit analysis for mitigating controls
B. Recommend risk acceptance to the business owner
C. Develop and implement a plan to mitigate the identified risk
D. Evaluate and prioritize the identified risk
Answer: (SHOW ANSWER)
The best first step is to evaluate and prioritize the risk to determine the appropriate treatment strategy before implementing mitigation.
"Once risks are identified, they should be evaluated and prioritized to determine the best response (mitigation, transfer, acceptance, or avoidance)."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*
ISACA practice questions confirm the need for evaluation and prioritization before taking further action.

NEW QUESTION: 186
Which of the following BEST illustrates residual risk within an organization?
A. Balanced scorecard
B. Risk management framework
C. Business impact analysis (BIA)
D. Heat map
Answer: (SHOW ANSWER)

NEW QUESTION: 187
The PRIMARY objective of timely declaration of a disaster is to:
A. ensure engagement of business management in the recovery process.
B. assess and correct disaster recovery process deficiencies.
C. protect critical physical assets from further loss.
D. ensure the continuity of the organization's essential services.
Answer: (SHOW ANSWER)

The primary objective of timely declaration of a disaster is to ensure the continuity of the organization's essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan (DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

NEW QUESTION: 188
When evaluating cloud storage solutions, the FIRST consideration should be:
A. The service level agreement (SLA) for encryption keys
B. Alignment with the organization's data classification policy
C. How the organization's sensitive data will be transferred
D. The volume of data to be stored in the cloud
Answer: (SHOW ANSWER)
The first consideration when evaluating cloud storage solutions is alignment with the organization's data classification policy (B). CISM emphasizes that security requirements must be driven by data sensitivity and business value. Before assessing encryption methods, SLAs, or data transfer mechanisms, the organization must determine what type of data will be stored and what protection level is required. Data classification informs confidentiality, integrity, availability, privacy, and regulatory requirements. Evaluating SLAs (A) or transfer methods (C) without understanding data sensitivity risks misalignment with governance and compliance obligations. Data volume (D) is an operational consideration, not a security driver.
References: ISACA CISM Review Manual (Risk management-data classification, cloud risk evaluation); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 189
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?
A. Patch management files
B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs
Answer: (SHOW ANSWER)
Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files are essential to recover a compromised system that needs a complete rebuild, as they can help

to restore the functionality, security, and performance of the system. Without patch management files, the system may not be able to run properly or securely, and may expose the organization to further risks or vulnerabilities. Network system logs, configuration management files, and intrusion detection system (IDS) logs are also important for recovering a compromised system, but they should be considered after patch management files. Network system logs can help to identify the source and scope of the attack, configuration management files can help to restore the original settings and policies of the system, and IDS logs can help to detect any malicious activities or anomalies on the system. References = CISM Review Manual, 16th Edition, pages 193-1941; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 672

NEW QUESTION: 190

Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

A. Intrusion detection

B. Log monitoring

C. Patch management

D. Antivirus software

Answer: (SHOW ANSWER)

= Patch management is the process of applying updates to software and hardware systems to fix security vulnerabilities and improve functionality. Patch management is one of the best ways to prevent the exploitation of system vulnerabilities, as it reduces the attack surface and closes the gaps that attackers can exploit. Patch management also helps to ensure compliance with security standards and regulations, and maintain the performance and availability of systems.

Intrusion detection is the process of monitoring network or system activities for signs of malicious or unauthorized behavior. Intrusion detection can help to detect and respond to attacks, but it does not prevent them from happening in the first place. Log monitoring is the process of collecting, analyzing and reviewing log files generated by various systems and applications. Log monitoring can help to identify anomalies, errors and security incidents, but it does not prevent them from occurring. Antivirus software is the program that scans files and systems for viruses, malware and other malicious code. Antivirus software can help to protect systems from infection, but it does not prevent the exploitation of system vulnerabilities that are not related to malware.

Therefore, patch management is the best security process to prevent the exploitation of system vulnerabilities, as it addresses the root cause of the problem and reduces the risk of compromise.

References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 204.

NEW QUESTION: 191

An organization has decided to implement an Internet of Things (IoT) solution to remain competitive in the market. Which of the following should information security do FIRST?

A. Recalculate risk profile

B. Implement compensating controls
C. Reassess risk tolerance levels
D. Update the security architecture
Answer: (SHOW ANSWER)
When introducing new technologies, the first step is to recalculate the risk profile to identify any new or changed risks.
"The implementation of new technologies should trigger a review of the risk profile to identify and address new exposures."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis*

NEW QUESTION: 192
An organization has updated its business goals in the middle of the fiscal year to respond to changes in market conditions. Which of the following is MOST important for the information security manager to update in support of the new goals?
A. Information security threat profile
B. Information security policy
C. Information security strategy
D. Information security objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 193
Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a public-facing web server?
A. Execution of unauthorized commands
B. Prevention of authorized access
C. Defacement of website content
D. Unauthorized access to resources
Answer: (SHOW ANSWER)
Prevention of authorized access is the greatest threat posed by a distributed denial of service (DDoS) attack on a public-facing web server because it prevents legitimate users or customers from accessing the web services or resources, causing disruption, dissatisfaction, and potential loss of revenue or reputation. Execution of unauthorized commands is not a threat posed by a DDoS attack, but rather by a remote code execution (RCE) attack. Defacement of website content is not a threat posed by a DDoS attack, but rather by a web application attack. Unauthorized access to resources is not a threat posed by a DDoS attack, but rather by a brute force attack or an authentication bypass attack. References:
https://www.isaca.org/resources/isaca-journal/issues
/2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016
/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 194
Which of the following processes should be done NEXT after completing a business impact analysis (BIA)?
A. Develop the requirements for the incident response plan
B. Develop a business continuity plan (BCP)
C. Evaluate the disaster recovery plan (DRP)
D. Identify resources for business recovery
Answer: (SHOW ANSWER)
After completing a business impact analysis, the next step is to identify resources for business recovery. The BIA identifies critical business processes, recovery priorities, impacts over time, recovery time objectives, and recovery point objectives. Once these requirements are known, the organization must determine the resources needed to meet them, such as personnel, facilities, technology, data, applications, vendors, and alternate processing capabilities. Developing a business continuity plan occurs after recovery requirements and resources are understood. Evaluating the disaster recovery plan would generally occur after plans have been developed and tested. Developing requirements for the incident response plan is related to incident management, but it is not the next step after a BIA in continuity planning. CISM program management emphasizes that BIA outputs drive recovery strategy development, and resource identification is a necessary bridge between impact analysis and actionable continuity plans. Therefore, identifying resources for business recovery is the appropriate next activity after the BIA.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - BIA outputs and continuity strategy development ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 195
Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?
A. Determine the final root cause of the incident.
B. Remove all instances of the incident from the network.
C. Mitigate exploited vulnerabilities to prevent future incidents.
D. Isolate affected systems to prevent the spread of damage.
Answer: (SHOW ANSWER)
Isolating affected systems limits the damage and prevents the incident from impacting other parts of the organization.
"During containment, the primary objective is to isolate affected systems to prevent further damage."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Process*

NEW QUESTION: 196
The effectiveness of an incident response team will be GREATEST when:
A. the incident response process is updated based on lessons learned,
B. the incident response team meets on a regular basis to review log files
C. the incident response team members are trained security personnel,
D. incidents are identified using a security information and event monitoring (SIEM) system.
Answer: A (LEAVE A REPLY)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 197
Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?
A. Residual risk
B. Regulatory requirements
C. Risk tolerance
D. Control objectives
Answer: (SHOW ANSWER)
The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance. References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 198
An organization recently identified a significant risk related to data exfiltration, and the information security manager is asked to quickly address this issue. The security team suggests a number of different security controls. Which of the following is the BEST approach for selecting controls to manage the risk?
A. Implement controls recommended by an industry-recognized security framework.

B. Assess the effectiveness of each control in reducing residual risk.
C. Prioritize the controls based on ease of implementation and resource availability.
D. Choose the most economical controls for risk mitigation based on a cost-benefit analysis.
Answer: (SHOW ANSWER)
The best approach for selecting security controls is to assess the effectiveness of each control in reducing residual risk (B). CISM emphasizes that control selection must be risk-based and outcome-focused, with the primary objective of reducing risk to within the organization's defined risk appetite. When multiple controls are available, the information security manager should evaluate how well each option mitigates the identified risk-specifically data exfiltration-and determine the resulting residual risk after implementation.
Implementing controls solely because they are recommended by a framework (A) may not adequately address the organization's specific threat scenario or business context. Prioritizing controls based on ease of implementation or available resources (C) shifts focus away from risk reduction and may result in insufficient protection. Cost-benefit analysis (D) is an important supporting activity, but in CISM it is secondary to understanding risk reduction effectiveness.
CISM guidance consistently states that security controls should be selected based on their ability to reduce risk exposure in a measurable and meaningful way, ensuring alignment with business objectives, risk tolerance, and governance expectations.
References:
ISACA CISM Review Manual, Information Risk Management - risk treatment and control selection
ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

NEW QUESTION: 199
Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?
A. Demonstrating the program's value to the organization
B. Discussing governance programs found in similar organizations
C. Providing the results of external audits
D. Providing examples of information security incidents within the organization
Answer: (SHOW ANSWER)
The best way to obtain senior management support for an information security governance program is to demonstrate the program's value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. References:
* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process

* https://www.sans.org/white-papers/992/
* https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for-your- security-program.html

NEW QUESTION: 200

Freecram.net

Which of the following would be the BEST way for an information security manager to improve the effectiveness of an organization's information security program?

A. Focus on addressing conflicts between security and performance.
B. Collaborate with business and IT functions in determining controls.
C. Include information security requirements in the change control process.
D. Obtain assistance from IT to implement automated security cantrals.
Answer: (SHOW ANSWER)
The best way for an information security manager to improve the effectiveness of an organization's information security program is to collaborate with business and IT functions in determining controls.
Collaboration is a key factor for ensuring that the information security program is aligned with the organization's business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program.
Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions.
Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance, and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.
Including information security requirements in the change control process © is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security

requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.
Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy Development, Subsection: Collaboration, page 24-251

NEW QUESTION: 201
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?
A. Updated security policies
B. Defined security standards
C. Threat intelligence
D. Regular antivirus updates
Answer: B (LEAVE A REPLY)
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information

security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.
Advanced Persistent Threats and Nation-State Actors 1
Book Review: Advanced Persistent Threats 2
Advanced Persistent Threat (APT) Protection 3
Establishing Advanced Persistent Security to Combat Long-Term Threats 4 What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION: 202
Which of the following is MOST important for an organization to have in place to determine the effectiveness of information security governance?
A. Program metrics
B. Key risk indicators (KRIs)
C. Risk register
D. Security strategy
Answer: (SHOW ANSWER)
Program metrics measure the effectiveness of governance processes and provide a basis for continuous improvement and informed decision-making.
"Metrics are essential for evaluating governance performance, demonstrating effectiveness, and identifying areas for improvement."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Monitoring and Metrics* ISACA's practice questions confirm that program metrics are key to evaluating governance effectiveness.

NEW QUESTION: 203
Which of the following is the MOST appropriate metric to demonstrate the effectiveness of information security controls to senior management?
A. Downtime due to malware infections
B. Number of security vulnerabilities uncovered with network scans
C. Percentage of servers patched
D. Annualized loss resulting from security incidents

Answer: (SHOW ANSWER)
Annualized loss resulting from security incidents is the most appropriate metric to demonstrate the effectiveness of information security controls to senior management, as it quantifies the financial impact of security breaches on the organization's assets, operations, and reputation. This metric helps to communicate the value of security investments, justify the security budget, and prioritize the security initiatives based on the potential loss reduction. Annualized loss resulting from security incidents can be calculated by multiplying the annualized rate of occurrence (ARO) of an incident by the single loss expectancy (SLE) of an incident. ARO is the estimated frequency of an incident occurring in a year, and SLE is the estimated cost of an incident. For example, if an organization estimates that a ransomware attack may occur once every two years, and that each attack may cost $100,000 to recover, then the annualized loss resulting from ransomware attacks is $50,000 ($100,000 / 2).
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112; Key Performance Indicators for Security Governance, Part 1; Performance Measurement Guide for Information Security

NEW QUESTION: 204
Which of the following should be done FIRST after discovering a security incident within an AI system?
A. Notify internal stakeholders
B. Inform regulatory authorities
C. Update the board of directors
D. Report incident details to law enforcement
Answer: (SHOW ANSWER)
The correct answer is A because after discovering a security incident within an AI system, the first action should be to notify the appropriate internal stakeholders according to the incident response process. Internal stakeholders may include the incident response team, information security management, system owner, legal, privacy, compliance, business owner, and technical teams. Notifying internal stakeholders enables the organization to validate the incident, assess scope, contain the issue, preserve evidence, and determine whether external notification is required. Informing regulatory authorities may be necessary later if the incident involves reportable personal data, regulated systems, or legal notification thresholds. Updating the board of directors may be required for significant incidents, but not before initial internal response and assessment. Reporting to law enforcement may also be appropriate in certain circumstances, but only after internal evaluation and legal guidance. CISM incident management emphasizes structured escalation, internal coordination, impact analysis, and appropriate communication. Therefore, internal stakeholder notification is the correct first step.
Reference: CISM Information Security Incident Management; incident notification, escalation, AI system incident response, and stakeholder communication principles.

NEW QUESTION: 205

A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What should be done NEXT?

A. Update in accordance with the best business practices.

B. Perform a risk assessment of the current IT environment.

C. Gain an understanding of the current business direction.

D. Inventory and review current security policies.

Answer: (SHOW ANSWER)

The next step for the information security manager should be to inventory and review the current security policies to understand the existing security requirements, controls, and gaps. This will help to identify the areas that need to be updated, revised, or replaced to align with the current business needs and objectives, as well as the legal and regulatory requirements. Updating the policies in accordance with the best business practices, performing a risk assessment of the current IT environment, or gaining an understanding of the current business direction are important activities, but they should be done after reviewing the current security policies. References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Policies, Standards, Procedures and Guidelines, Subsection: Information Security Policies, Page 28.

NEW QUESTION: 206

The MOST important reason for having an information security manager serve on the change management committee is to:

A. identify changes to the information security policy.

B. ensure that changes are tested.

C. ensure changes are properly documented.

D. advise on change-related risk.

Answer: (SHOW ANSWER)

The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2.

The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and

implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.
The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes.
Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk.
References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION: 207
Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?
A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions
C. Effective protection of information assets

D. Optimized allocation of recovery resources

Answer: D (LEAVE A REPLY)

The explanation given in the manual is:

Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

NEW QUESTION: 208

Which of the following is MOST important to include in an information security status report to senior management?

A. Key risk indicators (KRIs)

B. Review of information security policies

C. Information security budget requests

D. List of recent security events

Answer: (SHOW ANSWER)

According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

NEW QUESTION: 209

An incident response team has established that an application has been breached. Which of the following should be done NEXT?

A. Maintain the affected systems in a forensically acceptable state

B. Conduct a risk assessment on the affected application

C. Inform senior management of the breach.

D. Isolate the impacted systems from the rest of the network

Answer: (SHOW ANSWER)

The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems. References:

https://www.crowdstrike.com/cybersecurity-101/incident-response/

https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security/

NEW QUESTION: 210

When developing an asset classification program, which of the following steps should be completed FIRST?

Freecram.net

A. Categorize each asset.

B. Create an inventory. &

C. Create a business case for a digital rights management tool.

D. Implement a data loss prevention (OLP) system.

Answer: (SHOW ANSWER)

Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified.

An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12.

Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12.

Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. References = 1:

CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4:

What is Data Loss Prevention (DLP)? - Definition from Techopedia4

NEW QUESTION: 211

Which of the following is the MOST important consideration when determining which type of failover site to employ?

A. Reciprocal agreements

B. Disaster recovery test results

C. Recovery time objectives (RTOs)

D. Data retention requirements

Answer: (SHOW ANSWER)

The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources. Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 212

Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To increase awareness of information security among key stakeholders

B. To facilitate a qualitative risk assessment following the BIA

C. To obtain input from as many relevant stakeholders as possible
D. To ensure the stakeholders providing input own the related risk
Answer: C (LEAVE A REPLY)

NEW QUESTION: 213
What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?
A. Define the issues to be addressed.
B. Perform a cost-benefit analysis.
C. Calculate the total cost of ownership (TCO).
D. Conduct a feasibility study.
Answer: (SHOW ANSWER)
The first step when developing a business case for a new intrusion detection system (IDS) solution is to define the issues to be addressed. A business case is a document that provides the rationale and justification for initiating a project or investment. It typically includes information such as the problem statement, the objectives, the alternatives, the costs and benefits, the risks and assumptions, and the expected outcomes. The first step in developing a business case is to define the issues to be addressed, which means identifying and describing the current situation, the problems or challenges faced by the organization, and the needs or opportunities for improvement. By defining the issues to be addressed, the information security manager can establish the scope and purpose of the business case, and provide a clear and compelling problem statement that explains why a new IDS solution is needed. The other options are not the first step when developing a business case for a new IDS solution, although they may be part of the subsequent steps. Performing a cost-benefit analysis is a step that involves comparing the costs and benefits of different alternatives, including the new IDS solution and the status quo. A cost-benefit analysis can help evaluate and justify the feasibility and desirability of each alternative, and support the decision-making process. Calculating the total cost of ownership (TCO) is a step that involves estimating the direct and indirect costs associated with acquiring, operating, maintaining, and disposing of an asset or a system over its entire life cycle. A TCO calculation can help determine the long-term financial implications of investing in a new IDS solution, and compare it with other alternatives. Conducting a feasibility study is a step that involves assessing the technical, operational, legal, and economic aspects of implementing a project or an investment. A feasibility study can help identify and mitigate any potential issues or risks that may affect the success of the project or investment, and provide recommendations for improvement

NEW QUESTION: 214
Which of the following is the BEST indication of an effective information security program?
A. Risk is treated to an acceptable level.
B. The number of security incidents reported by staff has increased.
C. Key risk indicators (KRIs) are established.

D. Policies are reviewed and approved by senior management.

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Step-by-Step Explanation:

An effective information security program aims to manage risks to acceptable levels while supporting business objectives.

* A. Risk is treated to an acceptable level: This is the BEST answer as it directly reflects the program's success in mitigating risks within the organization's tolerance levels.
* B. The number of security incidents reported by staff has increased: An increase in reported incidents might indicate improved awareness but does not necessarily reflect overall effectiveness.
* C. Key risk indicators (KRIs) are established: KRIs are important for monitoring risks but do not indicate whether risks are being effectively managed.
* D. Policies are reviewed and approved by senior management: While essential, this action alone does not demonstrate the program's effectiveness.

Reference: CISM Job Practice Area 2 (Risk Management) highlights the importance of risk treatment and its alignment with organizational risk tolerance.

NEW QUESTION: 215

A PRIMARY benefit of adopting an information security framework is that it provides:

A. credible emerging threat intelligence.

B. security and vulnerability reporting guidelines.

C. common exploitability indices.

D. standardized security controls.

Answer: (SHOW ANSWER)

A standardized security control is a set of rules, guidelines, or best practices that are designed to protect the confidentiality, integrity, and availability of information assets and systems. An information security framework is a collection of standardized security controls that are aligned with the organization's objectives, strategy, and risk appetite. Adopting an information security framework provides a primary benefit of ensuring consistency, efficiency, and effectiveness in the implementation and management of information security across the organization.

References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is an Information Security Framework?; Information Security Frameworks: What Are They and Why Do You Need One?

NEW QUESTION: 216

For event logs to be acceptable for incident investigation, which of the following is the MOST important consideration to establish chain of evidence?

A. Administrator log access

B. Available forensic tools

C. Centralized logging

D. Time clock synchronization

Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?
A. Embedding compliance requirements within operational processes
B. Engaging external experts to provide guidance on changes in compliance requirements
C. Performing periodic audits for compliance with legal and regulatory requirements
D. Assigning the operations manager accountability for meeting compliance requirements
Answer: A (LEAVE A REPLY)
Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.
Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2. Compliance requirements may vary depending on the industry, location, and nature of the organization2. Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

NEW QUESTION: 218
When an information security manager presents an information security program status report to senior management, the MAIN focus should be:
A. Key controls evaluation
B. Net present value
C. Security return on investment
D. Key performance indicators
Answer: (SHOW ANSWER)
The correct answer is D because senior management needs concise, business-relevant information showing whether the information security program is achieving its objectives. Key performance indicators are used to measure progress, performance, and effectiveness against defined security goals. A program status report should not focus primarily on technical control evaluation, financial net present value, or security return on investment alone. Those may be useful supporting details, but they do not provide the clearest overall view of program performance. In CISM terms, information security reporting to senior management should support governance, decision-making, accountability, and alignment with enterprise objectives. KPIs allow management to understand trends, identify underperforming areas, allocate resources, and determine whether the information security program continues to support business priorities. Key control evaluations are more detailed operational or assurance activities, while ROI and NPV are financial measures that may not fully represent security effectiveness.
Reference: CISM Information Security Program Development and Management; Information Security Governance reporting and metrics principles.

NEW QUESTION: 219
Which of the following has the GREATEST impact on the ability to successfully execute a disaster recovery plan (DRP)?
A. Conducting tabletop exercises of the plan
B. Updating the plan periodically
C. Communicating the plan to all stakeholders
D. Reviewing escalation procedures
Answer: (SHOW ANSWER)
The CISM Review Manual emphasizes that the success of a DRP (Disaster Recovery Plan) depends greatly on clear communication of the plan to all stakeholders. Stakeholders must be aware of their roles and responsibilities during an incident to ensure the plan can be effectively executed. While testing, updating, and reviewing the plan are also important, communication is critical to effective execution.
Reference:ISACA CISM Review Manual, 16th Edition, Page 250-251, "Disaster Recovery Planning - Key Success Factors".

NEW QUESTION: 220
Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?
Freecram.net
A. Cost of the attack to the organization
B. Location of the attacker
C. Method of operation used by the attacker
D. Details from intrusion detection system (IDS) logs
Answer: (SHOW ANSWER)
= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

NEW QUESTION: 221
An organization's human resources department is planning to migrate a legacy application to a new application in the cloud. What is the BEST way for the information security manager to support this effort?

A. Update the policies to add controls for protecting the data
B. Encrypt the data to the cloud so that the data is secure
C. Conduct a security assessment on the cloud provider
D. Conduct vulnerability scans on the cloud provider
Answer: C (LEAVE A REPLY)
The correct answer is C because before migrating a human resources application to the cloud, the information security manager should assess the cloud provider's security capabilities, control environment, compliance posture, data protection practices, incident response process, access management, privacy protections, and contractual commitments. Human resources applications often process sensitive personal and employment information, so third-party and cloud risks must be evaluated before migration. Updating policies may be necessary later, but it does not determine whether the provider can adequately protect the data. Encrypting data is important, but encryption alone does not address all cloud risks such as access control, availability, segregation, monitoring, legal jurisdiction, breach notification, and vendor operations. Conducting vulnerability scans on the cloud provider may not be permitted and would provide only a narrow technical view. CISM emphasizes due diligence and risk assessment when outsourcing or using third-party services.
Therefore, a security assessment of the cloud provider is the best way to support the migration securely.
Reference: CISM Information Risk Management; cloud risk, third-party assessment, due diligence, data protection, and vendor security principles.

NEW QUESTION: 222
An enterprise has decided to procure security services from a third-party vendor to support its information security program. Which of the following is MOST important to include in the vendor selection criteria?
A. Feedback from the vendor's previous clients
B. Alignment of the vendor's business objectives with enterprise security goals
C. The maturity of the vendor's internal control environment
D. Penetration testing against the vendor's network
Answer: (SHOW ANSWER)
The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor's business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise's information security program. The alignment of the vendor's business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.

The vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It's a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

NEW QUESTION: 223
Which of the following BEST minimizes information security risk in deploying applications to the production environment?
A. Integrating security controls in each phase of the life cycle
B. Conducting penetration testing post implementation
C. Having a well-defined change process
D. Verifying security during the testing process
Answer: (SHOW ANSWER)
= Integrating security controls in each phase of the life cycle is the best way to minimize information security risk in deploying applications to the production environment. This ensures that security requirements are defined, designed, implemented, tested, and maintained throughout the development process. Conducting penetration testing post implementation, having a well-defined change process, and verifying security during the testing process are all important activities, but they are not sufficient to address all the potential risks that may arise during the application life cycle. Penetration testing may reveal some vulnerabilities, but it cannot guarantee that all of them are identified and fixed. A change process may help to control and document the modifications made to the application, but it does not ensure that the changes are secure and do not introduce new risks. Verifying security during the testing process may help to validate the functionality and performance of the security controls, but it does not ensure that the security requirements are complete and consistent with the business objectives and the risk appetite of the organization. References = CISM Review Manual, 16th Edition, page 1121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462

NEW QUESTION: 224
A small organization with limited budget hires a new information security manager who finds the same IT staff member is assigned the responsibility of system administrator, security administrator, database administrator (DBA), and application administrator What is the manager's BEST course of action?
A. Maintain strict control over user provisioning activities.
B. Implement monitoring of IT administrator activities.
C. Formally document IT administrator activities.
D. Automate user provisioning activities.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225

Which of the following is the BEST course of action when using a web application that has known vulnerabilities?
A. Deploy host-based intrusion detection.
B. Install anti-spyware software.
C. Monitor application level logs.
D. Deploy an application firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which of the following should an organization do FIRST upon learning that a subsidiary is located in a country where civil unrest has just begun?
A. Assess changes in the risk profile.
B. Conduct security awareness training.
C. Activate the disaster recovery plan (DRP).
D. Invoke the incident response plan.
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 227
Which of the following is MOST important when designing security controls for new cloud-based services?
A. Evaluating different types of deployment models according to the associated risks
B. Understanding the business and IT strategy for moving resources to the cloud
C. Defining an incident response policy to protect data moving between onsite and cloud applications
D. Performing a business impact analysis (BIA) to gather information needed to develop recovery strategies
Answer: (SHOW ANSWER)
The most important factor when designing security controls for new cloud-based services is to understand the business and IT strategy for moving resources to the cloud. This will help to align the security controls with the business objectives, requirements, and risks, and to select the appropriate cloud service delivery and deployment models. The security controls should also be based on the shared responsibility model, which defines the roles and responsibilities of the cloud

service provider and the cloud customer in ensuring the security of the cloud environment. Evaluating different types of deployment models, defining an incident response policy, and performing a business impact analysis are also important activities, but they should be done after understanding the business and IT strategy.
References = CISM Review Manual, 16th Edition eBook1, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 141-142.

NEW QUESTION: 228
An information security manager is working to incorporate media communication procedures into the security incident communication plan. It would be MOST important to include:
A. a directory of approved local media contacts
B. pre-prepared media statements
C. procedures to contact law enforcement
D. a single point of contact within the organization
Answer: (SHOW ANSWER)
A single point of contact within the organization is the most important element to include when incorporating media communication procedures into the security incident communication plan because it helps to ensure a consistent and accurate message to the public and avoid confusion or misinformation. A single point of contact is a designated person who is authorized and trained to communicate with the media on behalf of the organization during a security incident. The single point of contact should coordinate with the incident response team, senior management, legal counsel, and public relations to prepare and deliver timely and appropriate statements to the media, as well as to respond to any inquiries or requests. A single point of contact also helps to prevent unauthorized or conflicting disclosures from other employees or stakeholders that may harm the organization's reputation or legal position. Therefore, a single point of contact within the organization is the correct answer.
References:
https://www.lifars.com/2020/09/communication-during-incident-response/
https://ifpo.org/resource-links/articles-and-reports/public-and-media-relations/planning-for-effective-media- relations-during-a-critical-incident/
https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan.

NEW QUESTION: 229
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?
A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan

Answer: (SHOW ANSWER)

The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability.

This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.

The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner.

The other choices are possible actions but not necessarily the first one.

A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

NEW QUESTION: 230

To improve the efficiency of the development of a new software application, security requirements should be defined:

Freecram.net

A. based on code review.

B. based on available security assessment tools.

C. after functional requirements.

D. concurrently with other requirements.

Answer: (SHOW ANSWER)

Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the organization, not on code review, security assessment tools, or functional requirements. References = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

NEW QUESTION: 231

Which of the following provides the BEST indication of the return on information security investment?

A. Increased annualized loss expectancy (ALE)

B. Increased number of reported incidents

C. Reduced annualized loss expectancy (ALE)

D. Decreased number of reported incidents

Answer: (SHOW ANSWER)

A reduction in annualized loss expectancy (ALE) demonstrates that implemented controls have effectively reduced the organization's exposure to risk.

"ALE reduction is a key indicator of the cost-effectiveness of security investments and the improvement of the risk posture."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Cost-Benefit Analysis*

NEW QUESTION: 232

Which of the following is the BEST indication of an effective information security awareness training program?

A. An increase in the frequency of phishing tests

B. An increase in positive user feedback

C. An increase in the speed of incident resolution

D. An increase in the identification rate during phishing simulations

Answer: D (LEAVE A REPLY)

An effective information security awareness training program should aim to improve the knowledge, skills and behavior of the employees regarding information security. One of the ways to measure the effectiveness of such a program is to conduct phishing simulations, which are mock phishing attacks that test the employees' ability to identify and report phishing emails. An increase in the identification rate during phishing simulations indicates that the employees have learned how to recognize and avoid phishing attempts, which is one of the common threats to information security. Therefore, this is the best indication of an effective information security awareness training program among the given options.

The other options are not as reliable or relevant as indicators of an effective information security awareness training program. An increase in the frequency of phishing tests does not necessarily mean that the employees are learning from them or that the tests are aligned with the learning objectives of the program. An increase in positive user feedback may reflect the satisfaction or engagement of the employees with the program, but it does not measure the actual learning outcomes or behavior changes. An increase in the speed of incident resolution may be influenced by other factors, such as the availability and efficiency of the incident response team, the severity and complexity of the incidents, or the tools and processes used for incident management. Moreover, the speed of incident resolution does not reflect the prevention or reduction of incidents, which is a more desirable goal of an information security awareness training program.

References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1001.

NEW QUESTION: 233

What should an information security manager verify FIRST when reviewing an information asset management program?

A. System owners have been identified.
B. Key applications have been secured.
C. Information assets have been classified.
D. Information assets have been inventoried.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, information asset classification is the first step in an information asset management program, as it provides the basis for determining the level of protection required for each asset. System owners, key applications and information asset inventory are subsequent steps that depend on the classification of the assets.
References = CISM Review Manual, 27th Edition, Chapter 1, Section 1.4.2, page 381.

NEW QUESTION: 234
Which of the following is the MOST important objective of a disaster recovery test?
A. All critical data is recovered within recovery time objectives
B. All critical systems are successfully tested
C. Errors are discovered in the disaster recovery strategy
D. The business gains assurance it can recover from a disaster
Answer: (SHOW ANSWER)
The correct answer is D because the primary purpose of disaster recovery testing is to provide assurance that the organization can recover critical services and continue business operations after a disruptive event. While recovering data within recovery time objectives is important, that is only one measurable component of the broader recovery capability. Testing all critical systems may also be useful, but the real business objective is not merely technical system restoration; it is confidence that business operations can be restored to an acceptable level. Discovering errors in the strategy is a valuable result of testing, but it is not the main objective. From a CISM perspective, recovery planning must support business resilience, risk management, and continuity objectives. A disaster recovery test validates whether people, processes, technology, dependencies, communications, and recovery procedures work together effectively. Therefore, the most important objective is to give the business assurance that it can recover from a disaster.
Reference: CISM Information Security Incident Management; disaster recovery, business continuity, recovery testing, and resilience principles.

NEW QUESTION: 235
Which of the following is MOST important for the information security manager to include when presenting changes in the security risk profile to senior management?
A. Performance measures for existing controls
B. Industry benchmarks
C. Security training test results
D. Number of false positives
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which of the following is MOST important for responding effectively to security breaches?
A. Incident classification
B. Chain of custody
C. Communication plan
D. Log monitoring
Answer: (SHOW ANSWER)
The correct answer is C because effective breach response requires timely, accurate, and coordinated communication among internal teams, management, legal, regulators, customers, service providers, and other affected stakeholders. A security breach can quickly become a business, legal, operational, and reputational issue. Without a defined communication plan, response activities may be delayed, inconsistent, or mishandled. Incident classification is important because it helps determine severity and response actions, but it is only part of the process. Chain of custody is essential when evidence may be used for legal or disciplinary action, but it does not by itself ensure effective breach response. Log monitoring helps detect or investigate incidents, but it is not the most important response element once a breach is confirmed. CISM incident management principles emphasize predefined communication, escalation, roles, responsibilities, and stakeholder notification. A communication plan helps ensure the right people receive the right information at the right time, supporting effective and coordinated breach response.
Reference: CISM Information Security Incident Management; breach response, communication planning, stakeholder notification, and escalation principles.

NEW QUESTION: 237
Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?
A. Escalation processes
B. Technological capabilities
C. Recovery time objective (RTO)
D. Security audit reports
Answer: (SHOW ANSWER)
Escalation processes ensure that the provider and the organization can coordinate quickly and effectively during incidents.
"A clearly defined escalation process ensures that incidents are handled swiftly and with the appropriate level of authority, particularly when working with cloud service providers."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Cloud and Outsourced Incident Response* ISACA practice questions reinforce that escalation processes are critical when collaborating with third parties in incident management.

NEW QUESTION: 238

Which of the following is the MOST effective approach when reporting on the security program to business leadership?

A. Providing comprehensive security statistics

B. Reporting on industry security benchmarks

C. Outlining security audit results by line of business

D. Linking security to business strategy

Answer: (SHOW ANSWER)

The correct answer is D because business leadership needs security reporting that explains how the security program supports business objectives, risk management, compliance, resilience, and value delivery. Linking security to business strategy enables leadership to understand whether security investments and initiatives are helping the organization achieve its goals. Comprehensive security statistics may be too technical or operational unless translated into business impact. Industry benchmarks can provide useful context, but they do not necessarily reflect the organization's specific strategy, risk appetite, or priorities. Security audit results by line of business may help with accountability, but they are still only one source of assurance. CISM governance principles emphasize that security must be aligned with enterprise objectives and communicated in business-relevant terms. Effective reporting should support informed decision-making, prioritization, funding, and oversight. Therefore, the most effective approach is to connect the security program directly to business strategy.

Reference: CISM Information Security Governance; strategic alignment, business-focused reporting, governance metrics, and value delivery principles.

NEW QUESTION: 239

Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

A. Publish adopted information security standards.

B. Perform annual information security compliance reviews.

C. Implement an information security governance framework.

D. Define penalties for information security noncompliance.

Answer: (SHOW ANSWER)

The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can

embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

NEW QUESTION: 240

Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered the MOST significant exposure?

Freecram.net

A. Proxy server
B. Mail relay server
C. Database server
D. Application server
Answer: (SHOW ANSWER)

NEW QUESTION: 241

Which of the following is the BEST way to improve an organization's ability to detect and respond to incidents?
A. Perform a security gap analysis.
B. Conduct a business impact analysis (BIA).
C. Conduct periodic awareness training.
D. Perform network penetration testing.
Answer: C (LEAVE A REPLY)
The best way to improve an organization's ability to detect and respond to incidents is to conduct periodic awareness training (C). From a CISM incident management perspective, people are often the first line of detection. Employees, help desk staff, and operational personnel are frequently the first to notice unusual behavior, system anomalies, phishing attempts, or policy violations. Regular awareness training equips them with the knowledge to recognize indicators of compromise and escalate incidents promptly, which directly improves both detection and response times.
A security gap analysis (A) identifies deficiencies in controls but does not improve real-time detection or response capability. A business impact analysis (B) focuses on prioritizing recovery and resilience, not incident identification or handling. Network penetration testing (D) is a preventive and diagnostic activity that helps identify vulnerabilities but does not enhance operational response once an incident occurs.
CISM emphasizes that effective incident management depends on clear roles, defined escalation paths, and continuous awareness across the organization. Periodic training reinforces incident reporting criteria, response procedures, and accountability, thereby strengthening the organization's overall incident detection and response capability.

References:
ISACA CISM Review Manual, Information Security Incident Management - incident detection, response readiness, and awareness ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 242
Which of the following provides the GREATEST assurance that existing controls meet compliance requirements?
A. Engaging independent audits
B. Establishing compliance metrics
C. Reviewing security policies
D. Performing risk assessments
Answer: (SHOW ANSWER)
The correct answer is A because independent audits provide objective assurance that existing controls meet compliance requirements. Independent auditors can evaluate whether controls are appropriately designed, implemented, documented, and operating effectively against regulatory, contractual, or policy requirements.
Establishing compliance metrics is useful for monitoring trends and reporting status, but metrics may not provide sufficient independent validation. Reviewing security policies confirms whether requirements are documented, but it does not prove that controls are operating effectively.
Performing risk assessments helps identify and evaluate risk, but risk assessment is not the same as compliance assurance. In CISM governance, independent assurance is important because management needs reliable evidence that controls are effective and obligations are being met. Audits also help identify gaps, exceptions, and remediation needs. Because compliance requires evidence and objective evaluation, independent audits provide the greatest assurance among the listed options.
Reference: CISM Information Security Governance; independent assurance, compliance audits, control effectiveness, and governance oversight principles.

NEW QUESTION: 243
Which of the following is the PRIMARY objective of information asset classification?
A. Vulnerability reduction

B. Compliance management
C. Risk management
D. Threat minimization
Answer: (SHOW ANSWER)
The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security.
Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

NEW QUESTION: 244
Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?
A. Conducting periodic vulnerability assessments
B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework
Answer: (SHOW ANSWER)
The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or

outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

NEW QUESTION: 245
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?
A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.
Answer: D (LEAVE A REPLY)
The best course of action when the organization receives complaints from users that some of their files have been encrypted and they are receiving demands for money to decrypt the files is to initiate incident response.
This is because the organization is facing a ransomware attack, which is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and loss to the organization's operations, assets, and reputation. Therefore, the organization needs to quickly activate its incident response plan and team, which are designed to handle such security incidents in a coordinated, effective, and efficient manner. The incident response process involves the following steps1:
Preparation: The incident response team prepares the necessary resources, tools, and procedures to respond to the incident. The team also establishes the roles, responsibilities, and communication channels among the team members and other stakeholders.
Identification: The incident response team identifies the scope, source, and severity of the incident. The team also collects and preserves the relevant evidence and logs for further analysis and investigation.

Containment: The incident response team isolates the affected systems and networks to prevent the spread of the ransomware and limit the impact of the incident. The team also implements temporary or alternative solutions to restore the essential functions and services.
Eradication: The incident response team removes the ransomware and any traces of its infection from the affected systems and networks. The team also verifies that the systems and networks are clean and secure before restoring them to normal operations.
Recovery: The incident response team restores the affected systems and networks to normal operations. The team also decrypts or restores the encrypted data from backups or other sources, if possible. The team also monitors the systems and networks for any signs of recurrence or residual issues.
Lessons learned: The incident response team conducts a post-incident review to evaluate the effectiveness and efficiency of the incident response process and team. The team also identifies the root causes, lessons learned, and best practices from the incident. The team also recommends and implements the necessary improvements and corrective actions to prevent or mitigate similar incidents in the future.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, pages 229-2331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 45, page 432.

NEW QUESTION: 246
Which of the following is the BEST way to contain an SQL injection attack that has been detected by a web application firewall?
A. Force password changes on the SQL database.
B. Reconfigure the web application firewall to block the attack.
C. Update the detection patterns on the web application firewall.
D. Block the IPs from where the attack originates.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, one of the best ways to contain an SQL injection attack that has been detected by a web application firewall is to reconfigure the web application firewall to block the attack.
This means that the web application firewall should be updated with the latest detection patterns and rules that can identify and prevent SQL injection attacks. By doing so, the web application firewall can reduce the impact and damage of the attack, and prevent further exploitation of the vulnerable database1 The other options are not as effective as reconfiguring the web application firewall to block the attack. Force password changes on the SQL database is a reactive measure that does not address the root cause of the problem, and may cause data loss or corruption if not done properly. Updating the detection patterns on the web application firewall is a preventive measure that can help to detect SQL injection attacks, but it does not stop them from happening in the first place. Blocking IPs from where the attack originates is a defensive measure that can limit or stop some SQL injection attacks, but it does not protect all possible sources of malicious

traffic, and may also affect legitimate users or applications1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 32-33...

NEW QUESTION: 247
Which of the following should be the PRIMARY outcome of an information security program?
A. Strategic alignment
B. Risk elimination
C. Cost reduction
D. Threat reduction
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, strategic alignment is the primary outcome of an information security program1. Strategic alignment means that the information security program supports and is tailored to the organization's objectives and business strategy1. It also means that the information security program is aligned with other assurance functions, such as physical, human resources, quality, and IT1.
The CISM Review Manual (Digital Version) also states that strategic alignment is essential for achieving a competitive advantage, enhancing customer trust, reducing legal and regulatory risks, and improving organizational performance1. Strategic alignment requires effective communication and collaboration among all stakeholders, including senior management, information owners, information security managers, information security steering committees, and external partners1.
The CISM Exam Content Outline also covers the topic of strategic alignment in Domain 3 - Information Security Program Development and Management (33% exam weight)2. The subtopics include:
3.2.1 Information Security Strategy
3.2.2 Information Security Governance
3.2.3 Information Security Risk Management
3.2.4 Information Security Compliance
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 248
The PRIMARY purpose for deploying information security metrics is to:
A. compare program effectiveness to benchmarks.
B. ensure that technical operations meet specifications.
C. provide information needed to make decisions.
D. support ongoing security budget requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 249
A new type of ransomware has infected an organization's network. Which of the following would have BEST enabled the organization to detect this situation?
A. Use of integrated patch deployment tools

B. Periodic information security training for end users
C. Regular review of the threat landscape
D. Monitoring of anomalies in system behavior
Answer: D (LEAVE A REPLY)

NEW QUESTION: 250
Relationships between critical systems are BEST understood by
A. evaluating key performance indicators (KPIs)
B. performing a business impact analysis (BIA)
C. developing a system classification scheme
D. evaluating the recovery time objectives (RTOs)
Answer: (SHOW ANSWER)
The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

NEW QUESTION: 251
How does an incident response team BEST leverage the results of a business impact analysis (BIA)?
A. Assigning restoration priority during incidents
B. Determining total cost of ownership (TCO)
C. Evaluating vendors critical to business recovery
D. Calculating residual risk after the incident recovery phase
Answer: (SHOW ANSWER)
The incident response team can best leverage the results of a business impact analysis (BIA) by assigning restoration priority during incidents. A BIA is a process that identifies and evaluates the criticality and dependency of the organization's business functions, processes, and resources, and the potential impacts and consequences of their disruption or loss. The BIA results provide the basis for determining the recovery objectives, strategies, and plans for the organization's business continuity and disaster recovery. By using the BIA results, the incident response team can prioritize the restoration of the most critical and time-sensitive business functions, processes, and resources, and allocate the appropriate resources, personnel, and time to minimize the impact and duration of the incident.
Determining total cost of ownership (TCO) (B) is not a relevant way to leverage the results of a BIA, as it is not directly related to incident response. TCO is a financial metric that estimates the total direct and indirect costs of owning and operating an asset or a system over its lifecycle. TCO may be useful for evaluating the cost-effectiveness and return on investment of different security solutions or alternatives, but it does not help the incident response team to respond to or recover from an incident.

Evaluating vendors critical to business recovery © is also not a relevant way to leverage the results of a BIA, as it is not a primary responsibility of the incident response team. Evaluating vendors critical to business recovery is a part of the vendor management process, which involves selecting, contracting, monitoring, and reviewing the vendors that provide essential products or services to support the organization's business continuity and disaster recovery. Evaluating vendors critical to business recovery may be done before or after an incident, but not during an incident, as it does not contribute to the incident response or restoration activities.
Calculating residual risk after the incident recovery phase (D) is also not a relevant way to leverage the results of a BIA, as it is not a timely or effective use of the BIA results. Residual risk is the risk that remains after the implementation of risk treatment or mitigation measures. Calculating residual risk after the incident recovery phase may be done as a part of the incident review or improvement process, but not during the incident response or restoration phase, as it does not help the incident response team to resolve or contain the incident.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Business Impact Analysis, page 182-1831

NEW QUESTION: 252
An information security manager is updating the organization's incident response plan. Which of the following is the BEST way to validate that the process and procedures provided by IT and business units are complete, accurate, and known by all responsible teams?
A. Review the test objectives with stakeholders.
B. Conduct a data breach incident tabletop exercise.
C. Conduct an incident response plan survey.
D. Review data breach incident triage steps.
Answer: (SHOW ANSWER)
Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.
Reference:ISACA CISM Review Manual, 16th Edition, Page 295, "Testing and Validating Incident Response Plans".

NEW QUESTION: 253
An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance.
Which of the following would provide the MOST useful information for planning purposes? »
A. Results from a business impact analysis (BIA)
B. Deadlines and penalties for noncompliance
C. Results from a gap analysis

D. An inventory of security controls currently in place

Answer: (SHOW ANSWER)

Results from a gap analysis would provide the most useful information for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. A gap analysis is an assessment of the difference between an organization's current state of compliance and its desired level or standard. It is a process used to identify potential areas for improvement by comparing actual performance with expected performance. A gap analysis can help to prioritize the actions needed to close the gaps and comply with the regulatory requirements, as well as to estimate the resources and time required for each action1. The other options are not as useful as results from a gap analysis for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline.

Deadlines and penalties for noncompliance are important factors to consider, but they do not provide information on how to achieve compliance or what actions are needed2. Results from a business impact analysis (BIA) are useful for identifying the critical processes and assets that need to be protected, but they do not provide information on how to comply with the regulatory requirements or what actions are needed3. An inventory of security controls currently in place is useful for assessing the current state of compliance, but it does not provide information on how to comply with the regulatory requirements or what actions are needed4.

References: 3: Business impact analysis (BIA) - Wikipedia 2: Compliance Gap Analysis & Effectiveness Evaluation | SMS 1: What is Gap Analysis in Compliance | Scytale 4: Gap Analysis & Risk Assessment - Riddle Compliance

NEW QUESTION: 254

Which of the following is MOST important to include in an information security strategy?

A. Stakeholder requirements

B. Risk register

C. Industry benchmarks

D. Regulatory requirements

Answer: (SHOW ANSWER)

Stakeholder requirements are the most important to include in an information security strategy, as they reflect the business needs, objectives, and expectations of the organization and its key stakeholders. Stakeholder requirements also help to align the information security strategy with the enterprise governance and the organizational culture. Risk register, industry benchmarks, and regulatory requirements are important inputs for the information security strategy, but they are not the most important to include.

References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Task 1.12

NEW QUESTION: 255

An information security manager has recently been notified of potential security risks associated with a third- party service provider. What should be done NEXT to address this concern?
A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.
D. Determine compensating controls.
Answer: (SHOW ANSWER)
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third- party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION: 256
To help users apply appropriate controls related to data privacy regulation, what is MOST important to communicate to the users?
A. Results of penetration testing
B. Data classification policy
C. Features of data protection products
D. Data storage procedures
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 257
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?
A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.
Answer: (SHOW ANSWER)
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident

response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

NEW QUESTION: 258
A healthcare company is working with a virtual reality (VR) vendor to provide a training solution for customers of the organization's products. Which of the following is MOST important to include in the contract?
A. A requirement to encrypt the organization's data
B. A clause prohibiting reuse of the organization's data
C. A clause establishing the right to audit the vendor
D. A service level agreement (SLA) for uptime
Answer: C (LEAVE A REPLY)
The most important contractual provision is a clause establishing the right to audit the vendor. In CISM third- party governance, the organization remains accountable for protecting its information and must be able to obtain assurance that the vendor is meeting security, privacy, and compliance obligations. A right-to-audit clause gives the organization the ability to verify control effectiveness, review vendor practices, and assess whether contractual requirements are being followed. Encryption and prohibiting data reuse are important specific requirements, especially in healthcare where sensitive data may be involved, but they address only selected risks. Uptime SLAs address availability and do not provide broad assurance of security practices.
Because the question asks what is most important to include in the contract, CISM exam logic favors a governance mechanism that enables oversight and assurance over the entire vendor relationship. The right to audit supports accountability, compliance validation, and ongoing risk management, making it the strongest contractual safeguard.
References:
ISACA CISM Review Manual, Information Security Governance - third-party contracts, audit rights, and assurance ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 259
Which of the following will have the GREATEST influence on the successful adoption of an information security governance program?
A. Security policies
B. Control effectiveness
C. Security management processes
D. Organizational culture

Answer: (SHOW ANSWER)

Organizational culture is the set of shared values, beliefs, and norms that influence the way employees think, feel, and behave in the workplace. It affects how employees perceive the importance of information security, how they comply with security policies and procedures, and how they support security initiatives and goals. A strong security culture can foster a sense of ownership, responsibility, and accountability among employees, as well as a positive attitude toward security awareness and training. A weak security culture can lead to resistance, indifference, or hostility toward security efforts, as well as increased risks of human errors, negligence, or malicious actions. Therefore, organizational culture has the greatest influence on the successful adoption of an information security governance program, which requires the commitment and involvement of all levels of the organization. References = CISM Review Manual 15th Edition, page 30-31.

Learn more:

NEW QUESTION: 260

To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains

B. Risk reporting procedures

C. An audit committee consisting of mid-level management

D. Well-defined and approved controls

Answer: (SHOW ANSWER)

To support effective risk decision making, it is most important to have risk reporting procedures in place.

Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid- level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and

mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION: 261
An organization is considering using a third party to host sensitive archived data. Which of the following is MOST important to verify before entering into the relationship?
A. The vendor's data centers are in the same geographic region.
B. The encryption keys are not provisled to the vendor.
C. The vendor's controls are in line with the organization's security standards.
D. Independent audits of the vendor's operations are regularly conducted.
Answer: (SHOW ANSWER)
The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor's controls are in line with the organization's security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

NEW QUESTION: 262
An application is found to be out of compliance with a regulatory requirement. Of the following, who is MOST appropriate to own the associated risk?
A. The application owner
B. The compliance manager
C. The application developer
D. The process owner
Answer: (SHOW ANSWER)

The correct answer is D because information risk should be owned by the business or process owner responsible for the activity affected by the risk. When an application is out of compliance with a regulatory requirement, the associated risk is not merely technical; it may affect the business process, customers, legal obligations, operations, reporting, and organizational reputation. The process owner is best positioned to understand the business impact, make risk treatment decisions, and accept residual risk when appropriate. The application owner may be responsible for the application and may coordinate remediation, but the business process owner owns the business risk arising from noncompliance. The compliance manager advises on regulatory obligations and monitors compliance but does not usually own operational risk. The application developer may fix code or configuration issues but does not own the risk. CISM emphasizes that information security managers advise, while business or process owners are accountable for risk decisions. Therefore, the process owner is the most appropriate risk owner. Reference: CISM Information Risk Management; risk ownership, business accountability, regulatory noncompliance, and risk treatment responsibility.

NEW QUESTION: 263
To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?
A. Gap analysis results
B. Level of residual risk
C. Level of risk treatment
D. Configuration parameters
Answer: (SHOW ANSWER)
Level of residual risk is the amount of risk that remains after applying risk treatment options, such as avoidance, mitigation, transfer, or acceptance. The information security manager should compare the level of residual risk with the organization's risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its objectives. The comparison will help to determine whether the risk treatment options are sufficient, excessive, or inadequate, and whether further actions are needed to align the risk level with the risk appetite.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 49: "Residual risk is the risk that remains after risk treatment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 43: "Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value." CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "The information security manager should compare the residual risk with the risk appetite and determine whether the risk treatment options are sufficient, excessive, or inadequate."

NEW QUESTION: 264
What should be the PRIMARY objective of an information security policy?
A. To ensure alignment with industry best practices
B. To outline management expectations

C. To comply with regulatory requirements
D. To detail security procedures
Answer: (SHOW ANSWER)
The primary objective of an information security policy is to outline management expectations (B). In CISM governance, policies serve as high-level statements that define direction, intent, and accountability for information security. While alignment with best practices (A) and regulatory compliance (C) are important considerations, they are secondary to clearly communicating what management expects from the organization.
Detailing procedures (D) is not the role of policy; procedures translate policy into actionable steps. Clear policies establish authority and provide the foundation for standards, procedures, and enforcement.
References: ISACA CISM Review Manual (Governance-policy purpose and hierarchy); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 265
Of the following, who is BEST positioned to approve specific information security risk treatment options?
A. Risk owner
B. Information security manager
C. Head of risk management
D. Senior management
Answer: (SHOW ANSWER)
The risk owner (A) is best positioned to approve specific risk treatment options because they are accountable for the business process or asset affected by the risk and ultimately bear the consequences of that decision.
CISM clearly distinguishes between roles that advise on risk (e.g., information security manager, risk management function) and those that own and accept risk. Senior management (D) defines risk appetite and tolerance, but day-to-day treatment decisions are delegated to risk owners within those boundaries. Approving treatment options requires an understanding of operational impact, cost, and business value-making the risk owner the appropriate authority.
References: ISACA CISM Review Manual (Risk management-risk ownership, accountability, and risk response); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 266
Which of the following is the MOST critical factor for information security program success?
A. comprehensive risk assessment program for information security
B. The information security manager's knowledge of the business
C. Security staff with appropriate training and adequate resources
D. Ongoing audits and addressing open items
Answer: (SHOW ANSWER)
The explanation given in the manual is:

The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.
An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

NEW QUESTION: 267
Which of the following BEST enables an incident response team to determine appropriate actions during an initial investigation?
A. Procedures for incident triage
B. Historical data from past incidents
C. Feedback from affected departments
D. Technical capabilities of the team
Answer: (SHOW ANSWER)

NEW QUESTION: 268
Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?
A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider
Answer: D (LEAVE A REPLY)
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider. References:
https://www.wired.com/story/sequoia-hr-data-breach/

https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a- long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117- p599mr

NEW QUESTION: 269
Which of the following is MOST relevant to establishing security baselines?
A. Policies
B. Procedures
C. Guidelines
D. Standards
Answer: (SHOW ANSWER)
The correct answer is D because standards are most relevant to establishing security baselines. A security baseline defines the minimum required level of security configuration or control implementation for systems, applications, networks, or processes. Standards translate high-level policy requirements into mandatory, specific, measurable requirements. For example, a standard may define minimum password length, encryption requirements, secure configuration settings, logging requirements, patch timelines, or hardening requirements.
Policies state management intent and broad requirements, but they generally do not provide detailed technical baselines. Procedures provide step-by-step instructions for implementing or operating controls. Guidelines provide recommended practices, but they are usually advisory rather than mandatory. CISM governance recognizes the hierarchy of policy, standards, procedures, and guidelines, where standards define required minimum control expectations. Therefore, standards are the most relevant instrument for establishing security baselines across the organization.
Reference: CISM Information Security Governance; security baselines, standards, policy hierarchy, and control requirements principles.

NEW QUESTION: 270
Which of the following is the MOST critical activity for an information security manager to perform periodically throughout the term of a contract with an outsourced third party?
Freedram.net
A. Participatory disaster recovery testing
B. Comprehensive risk assessments
C. Service level agreement (SLA) updates
D. Financial alignment reviews
Answer: (SHOW ANSWER)
Performing comprehensive risk assessments (B) throughout the life of a third-party contract is the most critical activity because risk posture changes over time due to evolving threats, business changes, or control degradation. CISM emphasizes that third-party risk is not static and must be continuously assessed to ensure ongoing alignment with risk appetite. Disaster recovery testing (A) and SLA updates (C) are important but limited in scope. Financial reviews (D) focus on cost

rather than security risk. Periodic risk assessments enable timely identification of new risks and ensure appropriate mitigation or escalation.
References: ISACA CISM Review Manual (Governance-third-party risk lifecycle management); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 271
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.
Answer: (SHOW ANSWER)
= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =
1: CISM Review Manual 15th Edition, page 199-2004
2: CISM Practice Quiz, question 1011
3: Computer Security Incident Handling Guide5, page 2-3

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 272
Which of the following will ensure confidentiality of content when accessing an email system over the Internet?
A. Multi-factor authentication
B. Digital encryption
C. Data masking
D. Digital signatures
Answer: (SHOW ANSWER)

Digital encryption is the process of transforming data into an unreadable form using a secret key or algorithm.
Digital encryption will ensure the confidentiality of content when accessing an email system over the Internet, as it prevents unauthorized parties from intercepting, viewing, or modifying the email messages. Digital encryption can be applied to both the email content and the email transmission, using different methods such as symmetric encryption, asymmetric encryption, or hybrid encryption. Digital encryption can also provide other benefits such as authentication, integrity, and non-repudiation, depending on the encryption scheme and the use of digital signatures or certificates. References = CISM Review Manual 15th Edition, page 101, page 102.

NEW QUESTION: 273
Which of the following is MOST helpful to identify whether information security policies have been followed?
A. Directive controls
B. Corrective controls
C. Preventive controls
D. Detective controls
Answer: (SHOW ANSWER)

NEW QUESTION: 274
The PRIMARY goal when conducting post-incident reviews is to identify:
A. Additional cybersecurity budget needs
B. Weaknesses in incident response plans
C. Information to be shared with senior management
D. Individuals that need additional training
Answer: (SHOW ANSWER)
The core objective of a post-incident review (PIR) is to identify gaps and weaknesses in the response process.
This includes missteps, delays, communication failures, or policy limitations - all of which provide insight to improve future incident handling.
"Post-incident reviews focus on identifying root causes and areas for improvement to enhance the organization's preparedness for future incidents."
- CISM Review Manual 15th Edition, Chapter 4: Post-Incident Activities* Though training, reporting, and budgeting may follow, they are secondary outcomes of this process.

NEW QUESTION: 275
Which of the following is a PRIMARY benefit of managed security solutions?
A. Wider range of capabilities
B. Easier implementation across an organization
C. Greater ability to focus on core business operations

D. Lower cost of operations

Answer: (SHOW ANSWER)

Managed security solutions are services provided by external vendors that offer security expertise, resources, and tools to help organizations protect their information assets and systems. A primary benefit of managed security solutions is that they allow organizations to focus on their core business operations, while delegating the security tasks to the service provider. This can improve the efficiency and effectiveness of the organization, as well as reduce the complexity and cost of managing security internally. Managed security solutions can also provide a wider range of capabilities, easier implementation across an organization, and lower cost of operations, but these are not the primary benefits, as they may vary depending on the quality and scope of the service provider. References = CISM Review Manual, 16th Edition, ISACA, 2020, p. 841; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 3:
Information Security Program Management, ISACA2

NEW QUESTION: 276

An organization has identified a large volume of old data that appears to be unused. Which of the following should the information security manager do NEXT?

A. Consult the record retention policy.

B. Update the awareness and training program.

C. Implement media sanitization procedures.

D. Consult the backup and recovery policy.

Answer: (SHOW ANSWER)

The next thing that the information security manager should do after identifying a large volume of old data that appears to be unused is to consult the record retention policy. The record retention policy is a document that defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes. By consulting the record retention policy, the information security manager can determine if the old data is still required to be stored, archived, or disposed of, and how to do so in a secure and compliant manner.

References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention

policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

NEW QUESTION: 277
Which of the following has the MOST influence on the inherent risk of an information asset?
A. Risk tolerance
B. Net present value (NPV)
C. Return on investment (ROI)
D. Business criticality
Answer: (SHOW ANSWER)
Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes. References = CISM Review Manual,
16th Edition, page 971
Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

NEW QUESTION: 278
The PRIMARY purpose of vulnerability identification is to:
A. Remediate vulnerabilities before they are exploited
B. Discover control deficiencies
C. Provide vulnerability identifiers for risk reporting
D. Prioritize vulnerability remediation
Answer: A (LEAVE A REPLY)
The primary purpose of identifying vulnerabilities is to remediate them before they can be exploited by malicious actors. While risk reporting and prioritization are part of the overall process, the most immediate goal is remediation.
"Vulnerability assessments identify weaknesses that need to be addressed to reduce risk to acceptable levels and prevent potential exploits."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis This aligns with ISACA's official practice questions, where vulnerability identification directly aims to prevent exploitation.

NEW QUESTION: 279
Which of the following is the MOST important function of an information security steering committee?
A. Assigning data classifications to organizational assets
B. Developing organizational risk assessment processes
C. Obtaining multiple perspectives from the business
D. Defining security standards for logical access controls
Answer: (SHOW ANSWER)
An information security steering committee is a group of senior executives and managers from different business units and functions who provide strategic direction, oversight, and support for the information security program. The most important function of the committee is to obtain multiple perspectives from the business, as this helps to ensure that the information security program aligns with the business goals, needs, and culture, and that the security decisions reflect the interests and expectations of the stakeholders.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; Improve Security Governance With a Security Steering Committee2; The Role of the Corporate Information Security Steering Committee3

NEW QUESTION: 280
What is the PRIMARY benefit to an organization that maintains an information security governance framework?
Freecram.net
A. Resources are prioritized to maximize return on investment (ROI)
B. Information security guidelines are communicated across the enterprise_
C. The organization remains compliant with regulatory requirements.
D. Business risks are managed to an acceptable level.
Answer: (SHOW ANSWER)
According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.
Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.
According to the Certified Information Security Manager (CISM) Study Manual, "Information security governance provides a framework for managing and controlling information security

practices and technologies at an enterprise level. Its primary objective is to manage and reduce risk through a process of identification, assessment, and management of those risks." While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

NEW QUESTION: 281
Which of the following BEST mitigates the risk of information loss caused by a cloud service provider becoming insolvent?
A. Contractual provisions for the right to audit
B. Contractual provisions for data repatriation
C. Effective data loss prevention (DLP) controls
D. The purchase of cybersecurity insurance
Answer: (SHOW ANSWER)
The best mitigation for information loss caused by a cloud service provider becoming insolvent is contractual provisions for data repatriation. In CISM third-party and cloud governance, organizations must ensure they can retrieve their data in a usable format if a provider fails, terminates service, or becomes financially insolvent. Data repatriation clauses define how data will be returned, in what format, within what timeframe, and how securely it will be transferred or deleted from the provider environment. Right-to-audit clauses help assess controls but do not ensure data recovery if the provider fails. Data loss prevention controls reduce unauthorized data leakage, but they do not address provider insolvency or service termination. Cybersecurity insurance may offset some financial loss, but it does not restore access to critical information. Because data availability and portability are central cloud exit strategy requirements, contractual repatriation rights are the strongest control to mitigate the risk of losing access to information due to provider insolvency.
References:
ISACA CISM Review Manual, Information Security Governance - cloud service governance, exit strategy, and third-party contracts ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 282
Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?
A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats

Answer: (SHOW ANSWER)
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

NEW QUESTION: 283
Which of the following should include contact information for representatives of equipment and software vendors?
A. Information security program charter
B. Business impact analysis (BIA)
C. Service level agreements (SLAs)
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)
The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery.
Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. References:
https://www.isaca.org
/resources/isaca-journal/issues/2017/volume-2/business-continuity-management-lifecycle
https://www.isaca.
org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

NEW QUESTION: 284
Which of the following is the MOST important reason for logging firewall activity?
A. Firewall tuning
B. Incident investigation
C. Metrics reporting
D. Intrusion prevention
Answer: (SHOW ANSWER)

NEW QUESTION: 285

Which of the following BEST conveys minimum information security requirements to an organization in alignment with policies?

A. Standards

B. Procedures

C. Regulations

D. Baselines

Answer: (SHOW ANSWER)

Standards (A) best convey minimum information security requirements in alignment with organizational policies. In CISM governance, policies define management's intent and direction at a high level, while standards translate that intent into mandatory, enforceable minimum requirements that must be met across the organization. Standards ensure consistency and provide a clear benchmark against which compliance can be measured.

Procedures (B) describe how to perform specific tasks and are operational in nature; they are derived from standards and policies, not used to define minimum requirements. Regulations (C) are external mandates imposed by laws or regulatory bodies and are not internally defined mechanisms for conveying organizational security requirements. Baselines (D) typically represent a starting configuration or reference point for systems, often derived from standards, but they do not formally communicate organizational requirements on their own.

CISM clearly defines the hierarchy as policy # standards # procedures/guidelines, where standards play the critical role of establishing the minimum acceptable level of security needed to support governance objectives and ensure policy enforcement throughout the enterprise.

References:

ISACA CISM Review Manual, Information Security Governance - policy, standards, and procedures hierarchy ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 286

An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?

A. Document risk acceptances.

B. Revise the organization's security policy.

C. Assess the consequences of noncompliance.

D. Conduct an information security audit.

Answer: (SHOW ANSWER)

Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying

with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done. These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it. References = CISM Review Manual
2023, page 43 1; CISM Practice Quiz 2

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 287
A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:
A. incident has been confirmed.
B. incident has been contained.
C. potential incident has been logged.
D. incident has been mitigated.
Answer: (SHOW ANSWER)
= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by

the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.
The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset.
References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

NEW QUESTION: 288
A KEY consideration in the use of quantitative risk analysis is that it:
A. aligns with best practice for risk analysis of information assets.
B. assigns numeric values to exposures of information assets.
C. applies commonly used labels to information assets.
D. is based on criticality analysis of information assets.
Answer: (SHOW ANSWER)
A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent way, and to support the decision-making process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

NEW QUESTION: 289
Which of the following is the GREATEST benefit of information asset classification?
A. Helping to determine the recovery point objective (RPO)
B. Providing a basis for implementing a need-to-know policy
C. Supporting segregation of duties
D. Defining resource ownership
Answer: (SHOW ANSWER)

The greatest benefit of information asset classification is providing a basis for imple-menting a need-to-know policy. Information asset classification is a process of catego-rizing information based on its level of sensitivity and importance, and applying appro-priate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by:
*Defining the value and protection requirements of different types of information
*Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
*Establishing the roles and responsibilities of information owners, custodians, and users
*Enforcing access controls and encryption for the information
*Documenting the security policies and procedures for the information
By providing a basis for implementing a need-to-know policy, information asset classi-fication can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification.
Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud4.
De-fining resource ownership is not a benefit, but rather a component of information asset classification.
Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5. References: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3:
Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST : Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy
- UCI

NEW QUESTION: 290

Recommendations for enterprise investment in security technology should be PRIMARILY based on:

A. adherence to international standards
B. availability of financial resources
C. the organization s risk tolerance
D. alignment with business needs

Answer: (SHOW ANSWER)
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1, " Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance. " 1 The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security investments should be, as they can help protect the organization's assets and reputation from potential threats.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

NEW QUESTION: 291
Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?
A. Evaluate privacy technologies required for data protection.
B. Encrypt all personal data stored on systems and networks.
C. Update disciplinary processes to address privacy violations.
D. Create an inventory of systems where personal data is stored.
Answer: (SHOW ANSWER)
= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:
Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.
Assess the risks and impacts associated with the personal data, and the compliance requirements and obligations under the applicable data privacy regulations.
Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.
Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.

Monitor and review the performance and effectiveness of the data protection program, and report and resolve any data breaches or incidents.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Data Protection, pages 202-2051; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 71, page 662.

NEW QUESTION: 292
Which of the following would be MOST useful to help senior management understand the status of information security compliance?
A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Business impact analysis (BIA) results
D. Risk assessment results
Answer: (SHOW ANSWER)
Key performance indicators (KPIs) are measurable values that demonstrate how effectively an organization is achieving its key objectives and goals. KPIs can help senior management understand the status of information security compliance by providing quantifiable and relevant data on the performance and progress of the information security program and processes. KPIs can also help senior management to evaluate the effectiveness and efficiency of the information security controls and activities, identify strengths and weaknesses, and make informed decisions and adjustments. KPIs should be aligned with the organization's strategy, vision, and mission, and should be SMART (specific, measurable, achievable, relevant, and time- bound). Some examples of information security KPIs are: percentage of compliance with policies and standards, number of security incidents and breaches, mean time to detect and respond to incidents, percentage of systems and applications patched, number of security awareness trainings completed, etc.
Industry benchmarks, business impact analysis (BIA) results, and risk assessment results are not the most useful to help senior management understand the status of information security compliance, although they may provide some useful information or insights. Industry benchmarks are comparative measures of the performance or practices of other organizations in the same industry or sector. Industry benchmarks can help senior management to compare and contrast their own information security performance or practices with those of their peers or competitors, and identify gaps or opportunities for improvement. However, industry benchmarks may not reflect the specific goals, needs, or context of the organization, and may not be readily available or reliable. Business impact analysis (BIA) results are the outcomes of the process of analyzing the potential impacts of disruptive events on the organization's critical business functions and processes. BIA results can help senior management to understand the dependencies, priorities, and recovery objectives of the organization's business functions and processes, and to plan for business continuity and disaster recovery.
However, BIA results do not directly measure or indicate the status of information security compliance, and may not be updated or accurate. Risk assessment results are the outcomes of

the process of identifying, analyzing, and evaluating the information security risks that the organization faces. Risk assessment results can help senior management to understand the sources, causes, and consequences of information security risks, and to determine the appropriate risk responses and controls. However, risk assessment results do not directly measure or indicate the status of information security compliance, and may vary depending on the risk assessment methodology, criteria, and frequency. References = CISM Review Manual, 16th Edition, pages 47-481, 54-551, 69-701, 72-731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 832 Key performance indicators (KPIs) are metrics that measure the effectiveness and ef-ficiency of information security processes and activities. They help senior manage-ment understand the status of information security compliance by providing relevant, timely and accurate information on the performance of security controls, the level of risk exposure, the return on security investment and the progress toward security ob-jectives. KPIs can also be used to benchmark the organization's security performance against industry standards or best practices. KPIs should be aligned with the organiza-tion's strategic goals and risk appetite, and should be reported regularly to senior man-agement and other stakeholders. References:
*1 Key Performance Indicators for Security Governance, Part 1 - ISACA
*2 Key Performance Indicators for Security Governance, Part 2 - ISACA
*3 Compliance Metrics and KPIs For Measuring Compliance Effectiveness - Reciprocity
*4 14 Cybersecurity Metrics + KPIs You Must Track in 2023 - UpGuard

NEW QUESTION: 293
Which of the following BEST indicates that information assets are classified accurately?
A. Appropriate prioritization of information risk treatment
B. Increased compliance with information security policy
C. Appropriate assignment of information asset owners
D. An accurate and complete information asset catalog
Answer: A (LEAVE A REPLY)
The best indicator that information assets are classified accurately is appropriate prioritization of information risk treatment. Information asset classification is the process of assigning a level of sensitivity or criticality to information assets based on their value, impact, and legal or regulatory requirements. The purpose of information asset classification is to facilitate the identification and protection of information assets according to their importance and risk exposure. Therefore, if information assets are classified accurately, the organization can prioritize the information risk treatment activities and allocate the resources accordingly. The other options are not direct indicators of information asset classification accuracy, although they may be influenced by it. References = CISM Review Manual 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1031

NEW QUESTION: 294

Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?
A. It eliminates the need to maintain offsite facilities.
B. It lowers the annual cost to the business.
C. It transfers the risk associated with recovery to a third party.
D. It eliminates the need for the business to perform testing.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
Which of the following is the MOST common cause of cybersecurity breaches?
A. Lack of adequate password rotation
B. Human error
C. Abuse of privileged accounts
D. Lack of control baselines
Answer: (SHOW ANSWER)
Human error remains the leading cause of cybersecurity breaches, including mishandling data, misconfigurations, and falling for phishing attacks.
"Human error continues to be one of the most common causes of data breaches and security incidents."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Root Cause Analysis*

NEW QUESTION: 296
Management decisions concerning information security investments will be MOST effective when they are based on:
A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,
Answer: (SHOW ANSWER)
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION: 297

Which of the following should review and approve the objectives within an organization's information security framework?

A. Information security steering committee

B. Chief information security officer

C. Chief information officer

D. Information security manager

Answer: (SHOW ANSWER)

The correct answer is A because an information security steering committee provides cross-functional governance oversight and helps ensure that information security objectives align with enterprise goals.

Security framework objectives affect multiple business areas, including risk management, compliance, operations, technology, legal, and executive management. Therefore, approval should not rest solely with the information security manager, CISO, or CIO. The CISO and information security manager may develop and recommend objectives, while the CIO may provide technology leadership, but the steering committee is better positioned to review, prioritize, and approve objectives from an enterprise governance perspective. In CISM, effective information security governance requires senior-level direction, oversight, and alignment with business objectives. A steering committee also helps resolve conflicts, allocate resources, and ensure accountability across the organization. Because the framework establishes the direction and expectations for the security program, approval by the steering committee provides broader business representation and governance authority.

Reference: CISM Information Security Governance; steering committee, governance structure, security framework, and strategic alignment principles.

NEW QUESTION: 298

A data loss prevention (DLP) tool has flagged personally identifiable information (PII) during transmission.

Which of the following should the information security manager do FIRST?

A. Review and validate the rules within the DLP system.

B. Escalate the issue to senior management.

C. Validate the scope and impact with the business process owner.

D. Initiate the incident response plan.

Answer: (SHOW ANSWER)

NEW QUESTION: 299

Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software. What is the BEST way for the information security manager to help senior management understand the related risk?

A. Include the impact of the risk as part of regular metrics.

B. Recommend the security steering committee conduct a review.

C. Update the risk assessment at regular intervals

D. Send regular notifications directly to senior managers

Answer: (SHOW ANSWER)

Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact.

References: https://www.isaca.
org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security-investments

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of- your-information-security-management-system

NEW QUESTION: 300

Which of the following is MOST difficult to measure following an information security breach?

A. Reputational damage

B. Human resource costs

C. Regulatory sanctions

D. Replacement efforts

Answer: (SHOW ANSWER)

Reputational damage is often intangible, subjective, and hard to quantify, making it the most challenging aspect to measure.

"Reputation impact is difficult to quantify and may have long-term effects that are not immediately apparent."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis* ISACA practice questions highlight that reputational damage is uniquely challenging to measure accurately.

NEW QUESTION: 301

In information security governance, which of the following has PRIMARY responsibility for ensuring compliance with regulations?

A. Senior management

B. Enterprise risk management

C. Control owners

D. Legal counsel

Answer: (SHOW ANSWER)

The correct answer is A because senior management has primary responsibility for ensuring that the organization complies with applicable laws, regulations, contractual obligations, and governance requirements. While compliance tasks may be delegated to legal, risk, compliance, IT, and control owners, accountability remains with senior management. Enterprise risk management may help identify and manage regulatory risk, but it does not replace management accountability. Control owners are responsible for operating specific controls, but they are not accountable for overall regulatory compliance. Legal counsel advises on legal interpretation and obligations, but does not own enterprise compliance accountability. In CISM governance, senior management provides direction, resources, oversight, and accountability for information security and compliance. The information security manager supports this by implementing security programs, reporting risks, and advising on controls. However, the responsibility for ensuring regulatory compliance rests with senior leadership because compliance failures can affect the entire organization, including legal exposure, financial penalties, operational restrictions, and reputational harm.
Reference: CISM Information Security Governance; senior management accountability, regulatory compliance, governance oversight, and enterprise responsibility principles.

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 302
Which of the following processes is MOST important for the success of a business continuity plan (BCP)?
A. Including the board and senior management in plan reviews
B. Maintaining copies of the plan at the primary and recovery sites
C. Scheduling periodic internal and external audits
D. Involving all stakeholders in testing and training
Answer: (SHOW ANSWER)

NEW QUESTION: 303
An organization has identified IT failures in a call center application. Of the following, who should own this risk?
A. Chief executive officer (CEO)
B. Information security manager
C. Head of the IT department

D. Head of the call center
Answer: D (LEAVE A REPLY)

NEW QUESTION: 304
Which of the following has the GREATEST influence on the successful integration of information security within the business?
A. Organizational structure and culture
B. Risk tolerance and organizational objectives
C. The desired state of the organization
D. Information security personnel
Answer: (SHOW ANSWER)
The factor that has the greatest influence on the successful integration of information security within the business is organizational structure and culture because they determine how information security is organized, governed, and supported within the organization, and how information security roles and responsibilities are defined, assigned, and communicated across different levels and functions. Risk tolerance and organizational objectives are not very influential because they do not affect how information security is integrated within the business, but rather what information security aims to achieve or protect. The desired state of the organization is not very influential because it does not affect how information security is integrated within the business, but rather what the organization aspires to be or do. Information security personnel are not very influential because they do not affect how information security is integrated within the business, but rather who performs information security tasks or activities. References:
https://www.isaca.org/resources/isaca-journal/issues/2016
/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal
/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

NEW QUESTION: 305
Which of the following is the GREATEST benefit of performing a tabletop exercise of the business continuity plan (BCP)?
A. It allows for greater participation and planning from the business side.
B. It provides a low-cost method of assessing the BCP's completeness.
C. It identifies appropriate follow-up work to address shortcomings in the plan.
D. It helps in assessing the availability of compatible backup hardware.
Answer: (SHOW ANSWER)

NEW QUESTION: 306
The business value of an information asset is derived from:
A. the threat profile.
B. its criticality.
C. the risk assessment.

D. its replacement cost.

Answer: (SHOW ANSWER)

The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability (CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it.
References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

NEW QUESTION: 307

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

A. service level agreements (SLAs)

B. security requirements for the process being outsourced.

C. risk-reporting methodologies.

D. security metrics

Answer: (SHOW ANSWER)

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus primarily on defining security requirements for the process being outsourced.
Security requirements are the specifications of what needs to be done to protect the information assets from unauthorized access, use, disclosure, modification, or destruction. Security requirements should be aligned with the organization's risk appetite and business objectives, and should cover both technical and organizational aspects of the service delivery. Security requirements should also be clear, concise, measurable, achievable, realistic, and testable.
References = CISM Review Manual (Digital Version), Chapter
3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information.
They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are

essential to protect the information assets of the organization and to establish a clear and enforceable contractual relationship with the third party.
References:
*1 Outsourcing Strategies for Information Security: Correlated Losses and Security Exter-nalities - SpringerLink
*2 What requirements must outsourcing services comply with for the European market? - CBI
*3 Outsourcing cybersecurity: What services to outsource, what to keep in house - Infosec Institute
*4 BCFSA outsourcing and information security guidelines - BLG

NEW QUESTION: 308
Data classification is PRIMARILY the responsibility of:
A. the data custodian.
B. the security manager.
C. the data owner.
D. senior management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 309
Which of the following is the MOST critical consideration when shifting IT operations to an Infrastructure as a Service (IaaS) model hosted in a foreign country?
A. Labeling of data may help to ensure data is assigned to the correct cloud type.
B. Data may be stored in unknown locations and may not be easily retrievable.
C. There may be liabilities and penalties in the event of a security breach.
D. Laws and regulations of the origin country may not be applicable.
Answer: (SHOW ANSWER)

NEW QUESTION: 310
In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?
Freecram.net
A. Communicate regular reminders of the acceptable use policy
B. Include the topic of prohibited texting in security awareness training
C. Stop providing mobile devices until the organization is able to implement controls
D. Conduct a business impact analysis (BIA) and provide the report to management
Answer: (SHOW ANSWER)
In the absence of technical controls, the best way to reduce unauthorized text messaging is to include the topic of prohibited texting in security awareness training. CISM recognizes that when automated or technical enforcement is unavailable, user behavior must be influenced through targeted awareness and training.
Training is stronger than simple reminders because it can explain the policy requirement, business rationale, examples of prohibited behavior, consequences of noncompliance, and

proper alternatives. Regular reminders of the acceptable use policy may help reinforce expectations, but they are less effective than structured training. Stopping mobile device use would likely disrupt business and may not be proportionate to the risk.
Conducting a BIA is unrelated because the issue is user behavior and policy compliance, not continuity prioritization. CISM emphasizes that awareness and training programs should be tailored to specific roles, technologies, and behaviors. Therefore, incorporating prohibited texting into security awareness training is the best compensating measure when technical controls are not available.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - security awareness and acceptable use ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 311
What is the BEST way to address vulnerabilities associated with a recent increase in the number of zero-day attacks?
A. Implement USB port control throughout the company.
B. Implement automated antivirus updates.
C. Implement a behavior anomaly detection solution.
D. Develop a patching program.
Answer: (SHOW ANSWER)
Zero-day attacks exploit unknown vulnerabilities for which patches and signatures do not yet exist. Therefore, behavior anomaly detection (C) is the most effective approach because it focuses on abnormal system behavior, not known attack patterns. USB controls (A) address a specific threat vector but do not broadly mitigate zero-day risks. Automated antivirus updates (B) and patching programs (D) are essential baseline controls, but they are reactive and ineffective against unknown exploits. CISM emphasizes a risk-based, layered defense strategy, where advanced detection capabilities are used to identify and respond to emerging threats that bypass traditional controls. Behavior-based detection improves resilience against evolving and unknown attack techniques.
References: ISACA CISM Review Manual (Risk management-threat landscape, control selection, emerging risks); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 312
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?
A. To facilitate the continuous improvement of the IT organization
B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan
Answer: (SHOW ANSWER)

The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.
The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3:
Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION: 313
Business objectives and organizational risk appetite are MOST useful inputs to the development of information security:
A. risk assessments.
B. key performance indicators (KPIs).
C. standards.
D. strategy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 314
During which phase of an incident response plan is the root cause determined?
A. Recovery
B. Lessons learned
C. Containment
D. Eradication
Answer: (SHOW ANSWER)
The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 315

To help ensure that an information security training program is MOST effective its contents should be

A. focused on information security policy.

B. aligned to business processes

C. based on employees' roles

D. based on recent incidents

Answer: C (LEAVE A REPLY)

"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

NEW QUESTION: 316

When implementing a security policy for an organization handling personally identifiable information (PII); the MOST important objective should be:

A. strong encryption

B. regulatory compliance.

C. data availability.

D. security awareness training

Answer: (SHOW ANSWER)

Regulatory compliance is the most important objective when implementing a security policy for an organization handling personally identifiable information (PII) because it helps to ensure that the organization meets the legal and ethical obligations to protect the privacy and security of PII. PII is any information that can be used to identify, contact, or locate an individual, such as name, address, email, phone number, social security number, etc. PII is subject to various laws and regulations in different jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Failing to comply with these regulations can result in fines, lawsuits, reputational damage, or loss of trust. Therefore, regulatory compliance is the correct answer.

References:

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en

https://www.digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or- compromise

https://blog.rsisecurity.com/how-to-make-a-personally-identifiable-information-policy/

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest**

ExamDiscuss.com CISM dumps with Test Engine here:
https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 317
Before approving the implementation of a new security solution, senior management requires a business case.
Which of the following would BEST support the justification for investment?
A. The solution contributes to business strategy.
B. The solution improves business risk tolerance levels.
C. The solution improves business resiliency.
D. The solution reduces the cost of noncompliance with regulations.
Answer: (SHOW ANSWER)
The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 318
Following a risk assessment, an organization has made the decision to adopt a bring your own device (BYOD) strategy. What should the information security manager do NEXT?
A. Develop a personal device policy
B. Implement a mobile device management (MDM) solution
C. Develop training specific to BYOD awareness
D. Define control requirements
Answer: (SHOW ANSWER)
Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.
References:

* https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating- effective-policies-and-mitigating
* https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

NEW QUESTION: 319
Which of the following incident response phases involves actions to help safeguard critical systems while maintaining business operations?
A. Containment
B. Identification
C. Recovery
D. Preparation
Answer: (SHOW ANSWER)

NEW QUESTION: 320
Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?
Freecram.net
A. Disaster recovery drills
B. Penetration tests
C. Forensics certification
D. Tabletop exercises
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Of the following, who is in the BEST position to evaluate business impacts?
A. Senior management
B. Information security manager
C. IT manager
D. Process manager
Answer: (SHOW ANSWER)
The process manager is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The process manager has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the process manager is in the best position to evaluate the business impacts of a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The process manager can identify and quantify the potential losses, damages, or consequences that could result from the disruption or incident, such as revenue loss, customer dissatisfaction, regulatory non-compliance, reputational harm, or legal liability. The process manager can also provide input and feedback to the information security manager and the senior management on the business continuity and disaster recovery plans, the risk assessment and treatment, and the security

controls and measures that are needed to protect and recover the business processes and functions. References = CISM Review Manual 15th Edition, page 2301; CISM Practice Quiz, question 1302

NEW QUESTION: 322
Following a breach where the risk has been isolated and forensic processes have been performed, which of the following should be done NEXT?
A. Place the web server in quarantine.
B. Rebuild the server from the last verified backup.
C. Shut down the server in an organized manner.
D. Rebuild the server with relevant patches from the original media.
Answer: (SHOW ANSWER)
= After a breach where the risk has been isolated and forensic processes have been performed, the next step should be to rebuild the server from the last verified backup. This will ensure that the server is restored to a known and secure state, and that any malicious code or data that may have been injected or compromised by the attacker is removed. Rebuilding the server from the original media may not be sufficient, as it may not include the latest patches or configurations that were applied before the breach. Placing the web server in quarantine or shutting it down may not be feasible or desirable, as it may disrupt the business operations or services that depend on the server. Rebuilding the server from the last verified backup is the best option to resume normal operations while maintaining security. References = CISM Review Manual 15th Edition, page 118: "Recovery is the process of restoring normal operations after an incident. Recovery activities may include rebuilding systems, restoring data, applying patches, changing passwords, and testing functionality." Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2014 &
2015, snippet: "Restore from backup. If you have a backup of your system from before the breach, wipe your system clean and restore from backup. This will ensure that any backdoors or malware installed by the hackers are removed."

NEW QUESTION: 323
An organization's research department plans to apply machine learning algorithms on a large data set containing customer names and purchase history. The risk of personal data leakage is considered high impact.
Which of the following is the BEST risk treatment option in this situation?
A. Mitigate the risk by encrypting the customer names in the data set.
B. Mitigate the risk by applying anonymization on the data set.
C. Accept the risk, as the benefits exceed the potential consequences.
D. Transfer the risk by purchasing insurance.
Answer: (SHOW ANSWER)

NEW QUESTION: 324

Which of the following is ESSENTIAL to ensuring effective incident response?
A. Business continuity plan (BCP)
B. Cost-benefit analysis
C. Classification scheme
D. Senior management support
Answer: (SHOW ANSWER)
Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.
The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

NEW QUESTION: 325
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?
A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.
Answer: (SHOW ANSWER)
Defining information security requirements and processes is the FIRST thing that the information security manager should do to support the initiative of utilizing Software as a Service (SaaS) and selecting a vendor.
This is because information security requirements and processes provide the basis for evaluating and comparing the SaaS vendors and solutions, as well as for ensuring the alignment of the SaaS services with the organization's security objectives, policies, and standards. Information security requirements and processes should include aspects such as data protection, access control, encryption, authentication, authorization, audit, compliance, incident response, disaster recovery, and service level agreements12. Reviewing independent security assessment reports for each vendor (A) is a useful thing to do to support the initiative of utilizing SaaS and selecting a

vendor, but it is not the FIRST thing to do. Independent security assessment reports can provide valuable information about the security posture, practices, and performance of the SaaS vendors and solutions, such as their compliance with industry standards, frameworks, and regulations, their vulnerability and risk management, and their security testing and auditing results. However, reviewing independent security assessment reports should be done after defining the information security requirements and processes, which can help to determine the scope, criteria, and expectations for the security assessment12. Benchmarking each vendor's services with industry best practices (B) is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Benchmarking each vendor's services with industry best practices can help to measure and compare the quality, performance, and value of the SaaS vendors and solutions, as well as to identify the gaps, strengths, and weaknesses of the SaaS services. However, benchmarking each vendor's services with industry best practices should be done after defining the information security requirements and processes, which can help to select the relevant and appropriate industry best practices for the SaaS services12. Analyzing the risks and proposing mitigating controls © is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Analyzing the risks and proposing mitigating controls can help to identify and evaluate the potential threats, vulnerabilities, and impacts that may affect the security, availability, and reliability of the SaaS vendors and solutions, as well as to recommend and implement the necessary measures to reduce or eliminate the risks. However, analyzing the risks and proposing mitigating controls should be done after defining the information security requirements and processes, which can help to establish the risk appetite, tolerance, and criteria for the SaaS services12. References = 1: CISM Review Manual 15th Edition, page 82-831; 2: How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria - Gartner2

NEW QUESTION: 326

Which of the following is MOST important to emphasize when presenting information to gain senior management support for control enhancements?

A. Residual risk exposure

B. Threats against internal systems

C. Control gaps within defense-in-depth architecture

D. Recent data breaches in the same industry sector

Answer: (SHOW ANSWER)

Residual risk exposure (A) is the most important factor to emphasize because senior management is responsible for accepting or rejecting risk on behalf of the organization. CISM guidance stresses that executives are less concerned with technical details and more focused on what risk remains after controls are applied and whether it exceeds risk appetite. Threat details (B), architectural gaps (C), and industry breaches (D) can provide context, but they do not directly answer the key governance question: What level of risk does the organization still face? Presenting residual risk enables informed decision-making about whether additional controls are justified.

References: ISACA CISM Review Manual (Governance-risk reporting, executive decision-making); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 327
The PRIMARY benefit of introducing a single point of administration in network monitoring is that it:
A. reduces unauthorized access to systems.
B. promotes efficiency in control of the environment.
C. prevents inconsistencies in information in the distributed environment.
D. allows administrative staff to make management decisions.
Answer: (SHOW ANSWER)
A single point of administration in network monitoring is a centralized system that allows network administrators to manage and monitor the entire network from one location. A single point of administration can provide several benefits, such as:
Promoting efficiency in control of the environment: A single point of administration can simplify and streamline the network management tasks, such as configuration, troubleshooting, performance optimization, security updates, backup and recovery, etc. It can also reduce the time and cost of network maintenance and administration, as well as improve the consistency and quality of network services.
Reducing unauthorized access to systems: A single point of administration can enhance the network security by implementing centralized authentication, authorization and auditing mechanisms. It can also enforce consistent security policies and standards across the network, and detect and respond to any unauthorized or malicious activities.
Preventing inconsistencies in information in the distributed environment: A single point of administration can ensure the data integrity and availability by synchronizing and replicating the data across the network nodes.
It can also provide a unified view of the network status and performance, and facilitate the analysis and reporting of network data.
Allowing administrative staff to make management decisions: A single point of administration can support the decision-making process by providing relevant and timely information and feedback to the network administrators. It can also enable the administrators to implement changes and improvements to the network based on the business needs and objectives.
Therefore, the primary benefit of introducing a single point of administration in network monitoring is that it promotes efficiency in control of the environment, as it simplifies and streamlines the network management tasks and improves the network performance and quality. References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section
4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 205.

NEW QUESTION: 328

Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?

A. Establish key risk indicators (KRIs).

B. Use quantitative risk assessment methods.

C. Provide regular reporting on risk treatment to senior management

D. Require steering committee approval of risk treatment plans.

Answer: (SHOW ANSWER)

= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management.

However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter

2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION: 329

Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

A. Increase the frequency of system backups.

B. Review the mitigating security controls.

C. Notify staff members of the threat.

D. Assess the risk to the organization.

Answer: (SHOW ANSWER)

The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the

organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness.
The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat © is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. References = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

NEW QUESTION: 330

Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?

Freecram.net

A. Risk assessment results
B. Audit findings
C. Key risk indicators (KRIs)
D. Baseline controls
Answer: (SHOW ANSWER)
Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance.
Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are

an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs) are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. References = CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization." CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478:
"Baseline controls are the minimum security requirements that apply to all systems within the organization.
They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

NEW QUESTION: 331
How does an organization PRIMARILY benefit from the creation of an information security steering committee?
A. An increased focus on information security resource management
B. An increase in information security risk awareness
C. An increased alignment of information security with the business
D. An increased alignment with industry security trends that impact the business
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 332
In an organization that has an established social media policy, which of the following is the BEST way to reduce the risk associated with personally identifiable information disclosure?
A. Delivering regular training to employees about social media usage
B. Monitoring employees' social media usage for confidential content
C. Blocking social media sites on the corporate network
D. Controlling access to personally identifiable information within the organization
Answer: (SHOW ANSWER)
The correct answer is D because the most effective way to reduce disclosure risk is to limit access to personally identifiable information to only those individuals who have a legitimate

business need. If employees do not have unnecessary access to PII, the likelihood of accidental or intentional disclosure through social media is reduced at the source. Training is important and supports awareness, but it does not prevent inappropriate access to sensitive information.
Monitoring social media may detect some disclosures after they occur, but it is reactive and may also raise privacy and legal concerns. Blocking social media sites on the corporate network is limited because employees may still use personal devices or external networks.
CISM emphasizes risk-based controls, including access management, data protection, and least privilege.
Since the risk involves disclosure of PII, the best preventive control is restricting and controlling access to that information within the organization.
Reference: CISM Information Risk Management; privacy risk, data protection, access control, and least privilege principles.

NEW QUESTION: 333
When updating the information security policy to accommodate a new regulation, the information security manager should FIRST:
A. Review key risk indicators (KRIs)
B. Perform a gap analysis
C. Consult process owners
D. Update key performance indicators (KPIs)
Answer: B (LEAVE A REPLY)
A gap analysis identifies the differences between current practices and the new regulatory requirements, ensuring targeted and effective policy updates.
"Performing a gap analysis is critical to identify the areas where the current policy falls short of new regulatory requirements."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance* ISACA practice questions confirm that a gap analysis is the foundational step before engaging stakeholders or updating policies.

NEW QUESTION: 334
An organization has been penalized by regulatory authorities for failing to notify them of a major security breach that may have compromised customer data. Which of the following is MOST likely in need of review and updating to prevent similar penalties in the future?
A. Incident response training program
B. Incident communication plan
C. Information security policies and procedures
D. Business continuity plan (BCP)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 335

What should be the NEXT course of action when an information security manager has identified a department that is repeatedly not following the security policy?

A. Require department users to repeat security awareness training.

B. Introduce additional controls to force compliance with policy.

C. Report the policy violation to senior management.

D. Perform a vulnerability assessment on the systems within the department.

Answer: (SHOW ANSWER)

NEW QUESTION: 336

Company A, a cloud service provider, is in the process of acquiring Company B to gain new benefits by incorporating their technologies within its cloud services.

Which of the following should be the PRIMARY focus of Company A's information security manager?

A. The organizational structure of Company B

B. The cost to align to Company A's security policies

C. Company A's security architecture

D. Company B's security policies

Answer: (SHOW ANSWER)

According to the CISM Review Manual, the security architecture of an organization defines the security principles, standards, guidelines and procedures that support the information security strategy and align with the business objectives. When acquiring another company, the information security manager of the acquiring company should focus on ensuring that the security architecture of the acquired company is compatible with its own, or that any gaps or conflicts are identified and resolved.

References = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.2, page 751.

NEW QUESTION: 337

A new application has entered the production environment with deficient technical security controls. Which of the following is MOST Likely the root cause?

A. Inadequate incident response controls

B. Lack of legal review

C. Inadequate change control

D. Lack of quality control

Answer: (SHOW ANSWER)

Change control is the process of ensuring that changes to an information system are authorized, tested, documented and implemented in a controlled manner. Inadequate change control can result in deficient technical security controls, such as missing patches, misconfigurations, vulnerabilities or errors in the new application.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291

NEW QUESTION: 338

Which of the following is an information security manager's BEST course of action when a penetration test reveals a security exposure due to a firewall that is not configured correctly?
A. Ensure a plan with milestones is developed.
B. Implement a distributed denial of service (DDoS) control.
C. Engage the incident response team.
D. Define new key performance indicators (KPIs).
Answer: (SHOW ANSWER)
A penetration test is a proactive way to identify and remediate security vulnerabilities in a network. When a penetration test reveals a security exposure due to a firewall that is not configured correctly, the information security manager's best course of action is to ensure a plan with milestones is developed to address the issue.
This plan should include the root cause analysis, the corrective actions, the responsible parties, the deadlines, and the verification methods. This way, the information security manager can ensure that the security exposure is resolved in a timely and effective manner, and that the firewall configuration is aligned with the security policy and the business objectives.
References =
CISM Review Manual (Digital Version), page 193: "The information security manager should ensure that a plan with milestones is developed to address the issues identified during the penetration test." How to configure a network firewall: Walkthrough: "A good network firewall is essential. Learn the basics of configuring a network firewall, including stateful vs. stateless firewalls and access control lists in this episode of Cyber Work Applied." Which of the following is the BEST way to evaluate whether the information security program aligns with corporate governance?
A). Survey mid-level management.
B). Analyze industry benchmarks.
C). Conduct a gap analysis.
D). Review internal audit reports.

NEW QUESTION: 339
Unintentional behavior by an employee caused a major data loss incident. Which of the following is the BEST way for the information security manager to prevent recurrence within the organization?
A. Improve the security awareness training program.
B. Communicate consequences for future instances.
C. Enhance the data loss prevention (DLP) solution.
D. Implement compensating controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 340
Which of the following BEST demonstrates that an anti-phishing campaign is effective?
A. Improved staff attendance in awareness sessions

B. Decreased number of phishing emails received
C. Improved feedback on the anti-phishing campaign
D. Decreased number of incidents that have occurred
Answer: (SHOW ANSWER)
The ultimate goal of an anti-phishing campaign is to reduce the risk and impact of phishing attacks on the organization. Therefore, the most relevant and reliable indicator of the effectiveness of an anti-phishing campaign is the decreased number of incidents that have occurred as a result of phishing. This metric shows how well the employees have learned to recognize and report phishing emails, and how well the security controls have prevented or mitigated the damage caused by phishing.
References = Five Ways to Achieve a Successful Anti-Phishing Campaign; Don't click: towards an effective anti-phishing training. A comparative literature review; CISA, NSA, FBI, MS-ISAC Publish Guide on Preventing Phishing Intrusions

NEW QUESTION: 341
An organization has just updated its backup capability to a new cloud-based solution. Which of the following tests will MOST effectively verify this change is working as intended?
A. Tabletop testing
B. Parallel testing
C. Simulation testing
D. Black box testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 342
Which of the following is MOST helpful in determining whether a phishing email is malicious?
A. Reverse engineering
B. Threat intelligence
C. Sandboxing
D. Security awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 343
Which of the following is the BEST reason for delaying the application of a critical security patch?
A. Conflicts with the software development life cycle
B. Lack of vulnerability management
C. Resource limitations
D. Technology interdependencies
Answer: (SHOW ANSWER)
The best reason for delaying a critical security patch is technology interdependencies . CISM recognizes that patching must be risk-based, but also controlled to avoid creating operational outages or failures in dependent systems. Critical patches should generally be applied promptly;

however, if a patch may disrupt interconnected applications, infrastructure, or business-critical services, the organization may need to test, coordinate, and implement temporary compensating controls before deployment. Conflicts with the software development life cycle are not a strong reason to delay a critical security patch because emergency change processes should exist. Lack of vulnerability management is a program weakness, not a valid justification.
Resource limitations may explain a delay but do not represent a sound security rationale for accepting increased exposure. Technology interdependencies can create unacceptable availability or integrity impacts if not managed carefully. Therefore, delaying the patch may be justified only to ensure safe implementation while managing the interim risk through approved risk treatment and compensating controls.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - patch management, change control, and compensating controls ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 344
An information security policy was amended recently to support an organization's new information security strategy. Which of the following should be the information security manager's NEXT step?
A. Evaluate the alignment with business strategy
B. Review technical controls
C. Update standards and procedures
D. Refresh the security training program
Answer: (SHOW ANSWER)

NEW QUESTION: 345
Which of the following BEST enables an organization to maintain an appropriate security control environment?
A. Alignment to an industry security framework
B. Budgetary support for security
C. Periodic employee security training
D. Monitoring of the threat landscape
Answer: (SHOW ANSWER)
Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

NEW QUESTION: 346
Which of the following is MOST important when developing an information security strategy?
A. Engage stakeholders.

B. Assign data ownership.
C. Determine information types.
D. Classify information assets.
Answer: (SHOW ANSWER)
Engaging stakeholders is the most important step when developing an information security strategy, as it ensures that the strategy is aligned with the business objectives, risks, and needs of the organization.
Stakeholders include senior management, business units, IT staff, customers, regulators, and other relevant parties who have an interest or influence on the information security of the organization. By engaging stakeholders, the information security manager can gain their support, input, feedback, and buy-in for the strategy, as well as identify and prioritize the security requirements, expectations, and challenges.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 1

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 347
When defining a security baseline, it is MOST important that the baseline:
A. can vary depending on the security classification of systems.
B. is uniform for all assets of the same type.
C. is developed based on stakeholder consensus.
D. aligns to key risk indicators (KRIs).
Answer: B (LEAVE A REPLY)
A security baseline is a set of minimum security requirements for a system or asset type. The CISM Review Manual states that a baseline should be uniform for all assets of the same type to ensure consistency, enforceability, and ease of monitoring. This standardization supports effective compliance and security operations. While other factors can influence baseline adjustments, uniformity for similar asset types is most critical.
Reference:ISACA CISM Review Manual, 16th Edition, Page 207, "Establishing Security Baselines".

NEW QUESTION: 348
What is the PRIMARY objective of implementing standard security configurations?

A. Maintain a flexible approach to mitigate potential risk to unsupported systems.
B. Minimize the operational burden of managing and monitoring unsupported systems.
C. Control vulnerabilities and reduce threats from changed configurations.
D. Compare configurations between supported and unsupported systems.
Answer: (SHOW ANSWER)
The primary objective of implementing standard security configurations is to control vulnerabilities and reduce threats from changed configurations. Standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices. By implementing standard security configurations, the organization can ensure that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected. This can help to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should establish and implement standard security configurations for information systems and devices, and monitor and review the security configuration on a regular basis and take corrective actions when deviations or violations are detected" (p.
138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Control vulnerabilities and reduce threats from changed configurations is the correct answer because it is the primary objective of implementing standard security configurations, as it helps to maintain the security posture and functionality of information systems and devices, and to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks" (p. 63). Additionally, the article Standard Security Configurations from the ISACA Journal 2017 states that "standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices" and that "standard security configurations can help to control vulnerabilities and reduce threats from changed configurations by ensuring that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected" (p. 1)

NEW QUESTION: 349
What is the BEST way to reduce the impact of a successful ransomware attack?
A. Perform frequent backups and store them offline.
B. Purchase or renew cyber insurance policies.
C. Include provisions to pay ransoms ih the information security budget.
D. Monitor the network and provide alerts on intrusions.
Answer: (SHOW ANSWER)
Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems

without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself.
Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware.
Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

NEW QUESTION: 350

A recovery point objective (RPO) is required in which of the following?

A. Disaster recovery plan (DRP)
B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)

Answer: (SHOW ANSWER)

A recovery point objective (RPO) is required in a disaster recovery plan (DRP), because it indicates the earliest point in time to which it is acceptable to recover data after a disaster. It effectively quantifies the permissible amount of data loss in case of interruption. It is determined based on the acceptable data loss in case of disruption of operations1. A DRP is a document that defines the procedures, resources, and actions to restore the critical IT systems and data in the event of a disaster that affects the normal operations of the organization2. A DRP should include the RPO for each critical system and data, as well as the backup and restoration methods, frequency, and location to achieve the RPO3.
A RPO is not required in an information security plan, an incident response plan, or a business continuity plan (BCP), because these plans have different purposes and scopes. An information security plan is a document that defines the objectives, policies, standards, and guidelines for information security management in the organization4. An incident response plan is a document that defines the procedures, roles, and responsibilities for identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. A BCP is a document that defines the procedures, resources, and actions to ensure the continuity of the essential business functions and processes in the event of a disruption that affects the normal operations of the organization. These plans may include other metrics, such as recovery time objective (RTO), which is the amount of time after a disaster in which business operation is resumed, or resources are again available for use, but they do not require a RPO.
References
1: IS Disaster Recovery Objectives - RunModule
2: Information System Contingency Planning Guidance - ISACA

3: CISM Certified Information Security Manager - Question1411
4: CISM Review Manual, 16th Edition, ISACA, 2021, page 23.
5: CISM Review Manual, 16th Edition, ISACA, 2021, page 223.
6: CISM Review Manual, 16th Edition, ISACA, 2021, page 199.
7: RTO vs. RPO - What is the difference? - Advisera

NEW QUESTION: 351
A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?
A. Determine the required security controls for the new solution
B. Review the disaster recovery plans (DRPs) of the providers
C. Obtain audit reports on the service providers' hosting environment
D. Align the roles of the organization's and the service providers' stats.
Answer: (SHOW ANSWER)
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 352
Which of the following is the MOST important issue in a penetration test?
A. Having an independent group perform the test
B. Obtaining permission from audit
C. Performing the test without the benefit of any insider knowledge
D. Having a defined goal as well as success and failure criteria
Answer: (SHOW ANSWER)
The most important issue in a penetration test is having a defined goal as well as success and failure criteria.
A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors

or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach, as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

NEW QUESTION: 353
When selecting metrics to monitor the effectiveness of an information security program, it is MOST important for an information security manager to:
A. consider the organization's business strategy.
B. consider the strategic objectives of the program.
C. leverage industry benchmarks.
D. identify the program's risk and compensating controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 354
While classifying information assets an information security manager notices that several production databases do not have owners assigned to them What is the BEST way to address this situation?
A. Assign responsibility to the database administrator (DBA).
B. Review the databases for sensitive content.
C. Prepare a report of the databases for senior management.
D. Assign the highest classification level to those databases.
Answer: (SHOW ANSWER)
Information asset classification is the process of identifying, labeling, and categorizing information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to establish appropriate security controls, policies, and procedures for protecting the information assets from unauthorized access, use, disclosure, modification, or destruction. One of the key elements of information asset classification is assigning owners to each information asset. Owners are responsible for managing the information asset throughout its lifecycle, including defining its security requirements, implementing security controls, monitoring its usage and performance, reporting any incidents or breaches, and ensuring compliance with legal and regulatory obligations. Therefore, assigning responsibility to the database administrator (DBA) is the best way to address the situation where several production databases do not have owners assigned to them. References = CISM Review Manual 15th Edition1, page 256; Information Asset and Security Classification Procedure2.

NEW QUESTION: 355
Which of the following is the MOST effective control to prevent proliferation of shadow IT?
A. Install a solution to detect unlicensed software.
B. Conduct software audits.
C. Implement a software allow list.
D. Conduct periodic vulnerability scanning.
Answer: C (LEAVE A REPLY)
The most effective control to prevent the proliferation of shadow IT is implementing a software allow list.
From a CISM governance perspective, shadow IT represents the use of unauthorized applications and technologies outside established governance and approval processes, which increases risk exposure and undermines control effectiveness. CISM emphasizes that preventive controls are superior to detective controls when the objective is to stop undesirable behavior before it occurs.
A software allow list enforces policy by ensuring that only approved and authorized applications can be installed or executed, directly preventing users from introducing unapproved tools. In contrast, detecting unlicensed software (A) and conducting software audits (B) are detective controls that identify shadow IT only after it has already been deployed. Periodic vulnerability scanning (D) focuses on identifying technical weaknesses, not unauthorized software usage, and therefore does not address the root cause of shadow IT.
CISM guidance stresses aligning technical controls with governance policies to ensure consistent enforcement and risk reduction. Allow listing operationalizes policy requirements and supports management's intent by embedding control directly into system operation.
References:
ISACA CISM Review Manual, Information Security Governance - policy enforcement and preventive controls ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 356
Which of the following is the BEST approach to incident response for an organization migrating to a cloud- based solution?
A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.
Answer: (SHOW ANSWER)
The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles

and responsibilities, service level agreements, notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.
The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment.
References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-
192, 195-196, 199-200.
Cloud Incident Response Framework - A Quick Guide 2, pages 3-4, 6-7, 9-10.
CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

NEW QUESTION: 357
When establishing metrics for an information security program, the BEST approach is to identify indicators that:
A. reduce information security program spending.
B. support major information security initiatives.
C. reflect the corporate risk culture.
D. demonstrate the effectiveness of the security program.
Answer: (SHOW ANSWER)
Metrics for an information security program should be aligned with the security objectives and strategy, and should demonstrate how well the program is performing in terms of reducing risk, enhancing security posture, and supporting business goals. Metrics that support major information security initiatives, reflect the corporate risk culture, or reduce information security program spending may be useful, but they are not the best approach for establishing metrics for the entire program.
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112

NEW QUESTION: 358
Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?

A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents
Answer: C (LEAVE A REPLY)
Increasing accountability is the primary reason for ensuring clearly defined roles and responsibilities are communicated to users who have been granted administrative privileges due to specific application requirements. Administrative privileges grant users the ability to perform actions that can affect the security, availability and integrity of the application or system, such as installing software, modifying configurations, accessing sensitive data or granting access to other users. Therefore, users who have administrative privileges must be aware of their roles and responsibilities and the consequences of their actions. Communicating clearly defined roles and responsibilities to these users helps to establish accountability by setting expectations, defining boundaries, assigning ownership and enabling monitoring and reporting. Accountability also helps to deter misuse or abuse of privileges, ensure compliance with policies and standards, and facilitate incident response and investigation.
Clearer segregation of duties is a benefit of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Segregation of duties is a control that aims to prevent or detect conflicts of interest, errors, fraud or unauthorized activities by separating different functions or tasks among different users or groups. For example, a user who can create a purchase order should not be able to approve it. Segregation of duties helps to reduce the risk of unauthorized or inappropriate actions by requiring more than one person to complete a critical or sensitive process. However, segregation of duties alone does not ensure accountability, as users may still act in collusion or circumvent the control.
Increased user productivity is a possible outcome of ensuring clearly defined roles and responsibilities, but it is not the primary reason. User productivity refers to the efficiency and effectiveness of users in performing their tasks and achieving their goals. By communicating clearly defined roles and responsibilities, users may have a better understanding of their tasks, expectations and performance indicators, which may help them to work faster, smarter and better. However, user productivity is not directly related to the security risk of granting administrative privileges, and it may also depend on other factors, such as user skills, motivation, tools and resources.
Fewer security incidents is a desired result of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Security incidents are events or situations that compromise the confidentiality, integrity or availability of information assets or systems. By communicating clearly defined roles and responsibilities, users may be more aware of the security implications of their actions and the potential threats and vulnerabilities they may face, which may help them to avoid or prevent security incidents. However, fewer security incidents is not a guarantee or a measure of accountability, as users may still cause or experience security incidents due to human error, negligence, malicious intent or external factors. References = CISM Review Manual 15th Edition,

page 144 Effective User Access Reviews - ISACA1 CISM ITEM DEVELOPMENT GUIDE - ISACA2

NEW QUESTION: 359
When a critical system incident is reported, the FIRST step of the incident handler should be to:
A. Notify the appropriate parties
B. Determine the scope of the incident
C. Validate the incident
D. Power off the system
Answer: (SHOW ANSWER)
The correct answer is C because the first step after an incident is reported is to validate whether the reported event is actually an incident. Validation helps prevent unnecessary escalation, disruption, or incorrect response actions. The incident handler should confirm the event by reviewing available evidence, logs, alerts, user reports, system behavior, or other indicators. After validation, the handler can classify the incident, determine severity, assess scope, notify appropriate parties, and begin containment or eradication according to the incident response plan. Notifying parties before validation may cause confusion or unnecessary escalation. Determining scope is important, but it should occur after confirming that an incident exists. Powering off the system may destroy volatile evidence, disrupt business operations, or worsen the situation if done without analysis. CISM incident management principles require orderly identification, validation, classification, escalation, and response. Therefore, validating the incident is the correct first action for the incident handler.
Reference: CISM Information Security Incident Management; incident identification, validation, classification, escalation, and response handling principles.

NEW QUESTION: 360
Capacity planning would prevent:
A. file system overload arising from distributed denial of service (DDoS) attacks.
B. system downtime for scheduled security maintenance.
C. application failures arising from insufficient hardware resources.
D. software failures arising from exploitation of buffer capacity vulnerabilities.
Answer: (SHOW ANSWER)
Capacity planning is the process of estimating and allocating the required resources (such as CPU, memory, disk space, bandwidth, etc.) to meet the current and future demands of the information systems and applications. Capacity planning would prevent application failures arising from insufficient hardware resources, as it would ensure that the applications have enough resources to function properly and efficiently, and avoid performance degradation, errors, or crashes.
References = CISM Review Manual 2022, page 3081; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.92; What is Capacity Planning? Definition and Examples

NEW QUESTION: 361
Which of the following roles is BEST able to influence the security culture within an organization?
A. Chief information security officer (CISO)
B. Chief information officer (CIO)
C. Chief executive officer (CEO)
D. Chief operating officer (COO)
Answer: (SHOW ANSWER)
The CEO is the best able to influence the security culture within an organization because the CEO sets the tone and direction for the organization and has the authority and responsibility to ensure that the organization' s objectives are aligned with its strategy. The CEO can also communicate the importance and value of information security to all stakeholders and foster a culture of security awareness and accountability. The CISO, CIO and COO are important roles in information security management, but they do not have the same level of influence and authority as the CEO. References = CISM Review Manual, 16th Edition, page 221; CISM Exam Content Outline, Domain 1, Task 12 The Chief Information Security Officer (CISO) is responsible for leading and coordinating an organization's information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to information security, the CISO can help to create a security- aware culture within the organization.

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 362
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?
A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products
D. Unreliable delivery of hardware and software resources by a supplier
Answer: (SHOW ANSWER)
= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data.

The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page
189 1; CISM Practice Quiz 2

NEW QUESTION: 363
Which of the following is the FIRST step in developing a business continuity plan (BCP)?
A. Determine available resources.
B. Identify the applications with the shortest recovery time objectives (RTOs).
C. Identify critical business processes.
D. Determine the business recovery strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 364
An experienced information security manager joins a new organization and begins by conducting an audit of all key IT processes. Which of the following findings about the vulnerability management program should be of GREATEST concern?
A. The number of vulnerabilities identified exceeds industry benchmarks. D. Vulnerabilities are identified by internal staff rather than by external consultants.
B. Identified vulnerabilities are not logged and resolved in a timely manner.
C. Identified vulnerabilities are not published and communicated in awareness programs.
Answer: (SHOW ANSWER)

NEW QUESTION: 365
The resilience requirements of an application are BEST determined by:
A. A risk assessment
B. A business impact analysis (BIA)
C. A cost-benefit analysis
D. A threat assessment
Answer: (SHOW ANSWER)
A business impact analysis (BIA) (B) best determines application resilience requirements because it identifies criticality, maximum tolerable downtime, recovery time objectives (RTOs),

and recovery point objectives (RPOs) based on business impact. Resilience is fundamentally about the organization's ability to continue or rapidly restore critical business functions. Risk assessments (A) and threat assessments (D) identify risks and threat sources but do not define acceptable downtime or recovery priorities. Cost-benefit analysis (C) helps evaluate investment decisions but is secondary to understanding business impact. CISM clearly positions the BIA as the foundation for continuity, resilience, and recovery planning decisions, ensuring security and availability controls align with business priorities.
References: ISACA CISM Review Manual (Risk management-BIA, resilience, continuity planning); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 366
Which of the following BEST contributes to establishing an information security culture within an organization?
A. Conducting regular information security awareness initiatives
B. Obtaining executive approval of information security policy
C. Following industry best practices for information security
D. Incorporating information security requirements in the software development life cycle
Answer: (SHOW ANSWER)
The correct answer is A because a security culture is built through continuous reinforcement of expected behaviors across the organization. Regular information security awareness initiatives help employees understand threats, responsibilities, acceptable behavior, and how their daily actions affect organizational security. Executive approval of policy is important, but a policy alone does not create culture unless it is communicated, understood, and practiced. Following industry best practices may improve the security program, but it does not directly influence employee behavior throughout the organization. Incorporating security requirements into the software development life cycle is important for secure systems development, but it targets a specific process area rather than the entire organization. A strong information security culture requires awareness, communication, leadership support, and repeated behavioral reinforcement. From a CISM perspective, governance promotes a culture where information security is recognized as a business responsibility, not just a technical function. Regular awareness initiatives are therefore the best direct contributor among the options.
Reference: CISM Information Security Governance; security awareness, culture, and organizational behavior principles.

NEW QUESTION: 367
Which of the following is a PRIMARY responsibility of the information security goxernance function?
A. Administering information security awareness training
B. Defining security strategies to support organizational programs
C. Ensuring adequate support for solutions using emerging technologies
D. Advising senior management on optimal levels of risk appetite and tolerance

Answer: (SHOW ANSWER)
Defining security strategies to support organizational programs is a primary responsibility of the information security governance function, as it involves providing strategic direction for security activities and ensuring that objectives are achieved. According to ISACA, information security governance is a subset of corporate governance that provides guidance for aligning information security with business objectives, managing information security risks, and using information resources responsibly12.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12

NEW QUESTION: 368
An email digital signature will:
A. protect the confidentiality of an email message.
B. verify to recipient the integrity of an email message.
C. automatically correct unauthorized modification of an email message.
D. prevent unauthorized modification of an email message.
Answer: (SHOW ANSWER)
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References: https://support.microsoft.com/en-us/office/secure- messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com /searchsecurity/definition/digital-signature

NEW QUESTION: 369
Which of the following should an information security manager do FIRST when an evaluation reveals that required encryption for data in transit has not been implemented?
A. Determine the reason for noncompliance
B. Perform a business impact analysis
C. Report to senior management
D. Implement compensating controls
Answer: (SHOW ANSWER)
The correct answer is A because the information security manager should first determine why the required encryption control has not been implemented. Understanding the reason for noncompliance is necessary before selecting the appropriate corrective action. The issue may be

caused by technical limitations, lack of awareness, cost constraints, legacy systems, misconfiguration, project delay, undocumented exception, or business requirements. Performing a business impact analysis is not the first step because BIA is used mainly for continuity planning and impact analysis, not immediate control noncompliance investigation. Reporting to senior management may be necessary if the issue creates significant risk or remains unresolved, but reporting before understanding the cause may be premature. Implementing compensating controls may be appropriate if encryption cannot be implemented immediately, but the manager must first understand why the requirement was not met. CISM program management emphasizes control monitoring, exception management, root cause understanding, and risk-based remediation. Therefore, determining the reason for noncompliance is the correct first action.
Reference: CISM Information Security Program Development and Management; control compliance, exception management, remediation, and control monitoring principles.

NEW QUESTION: 370

An organization is planning to engage a third-party service provider to develop custom software. Which of the following would help to provide the GREATEST assurance of software security?

Pass4cram.net

A. Security training for the service provider's software development staff
B. Independent assessment against a relevant standard
C. Verification of certifications held by the individual developers
D. Review of the service provider's software development policies
Answer: (SHOW ANSWER)
An independent assessment against a relevant standard (B) provides the greatest assurance because it offers objective, third-party validation that security controls and development practices meet defined criteria.
Examples include assessments against secure development standards or recognized control frameworks.
Training (A), certifications (C), and policy reviews (D) are useful inputs, but they are indirect and do not confirm consistent, effective implementation. CISM emphasizes independent assurance for third-party risk management, especially when outsourcing high-risk activities such as custom software development.
Independent assessments reduce reliance on self-attestation and help validate governance, SDLC controls, and security testing practices.
References: ISACA CISM Review Manual (Third-party risk management, assurance, and program oversight); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 371
Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?
A. Increase in the number of reported security incidents
B. Increase in the frequency of security incident escalations
C. Decrease in the number of security incidents

D. Reduction in the impact of security incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 372
Which of the following would BEST justify spending for a compensating control?
A. Root cause analysis
B. Vulnerability assessment
C. Emerging risk trends
D. Risk analysis
Answer: D (LEAVE A REPLY)
A risk analysis (D) best justifies spending on a compensating control because it quantifies or qualifies risk exposure and residual risk, providing a business-based rationale for investment. CISM stresses that control decisions must be driven by risk, not by the existence of vulnerabilities alone. Root cause analysis (A) explains why an issue occurred, vulnerability assessments (B) identify weaknesses, and emerging trends (C) provide context-but only risk analysis connects threats, vulnerabilities, impact, and likelihood to justify expenditure.
References: ISACA CISM Review Manual (Risk management-risk evaluation and treatment); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 373
Which of the following is the PRIMARY role of an information security manager in a software development project?
A. To enhance awareness for secure software design
B. To assess and approve the security application architecture
C. To identify noncompliance in the early design stage
D. To identify software security weaknesses
Answer: (SHOW ANSWER)
The primary role of an information security manager in a software development project is to assess and approve the security application architecture. The security application architecture is the design and structure of the software application that defines how the application components interact with each other and with external systems, and how the application implements the security requirements, principles, and best practices. The information security manager is responsible for ensuring that the security application architecture is aligned with the organization's information security policies, standards, and guidelines, and that it meets the business objectives, functional specifications, and user expectations. The information security manager is also responsible for reviewing and evaluating the security application architecture for its completeness, correctness, consistency, and compliance, and for identifying and resolving any security issues, risks, or gaps. The information security manager is also responsible for approving the security application architecture before the software development project proceeds to the next phase, such as coding, testing, or deployment.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 80, page 742.

NEW QUESTION: 374
To improve an organization's information security culture, it is MOST important for senior management to:
A. Approve security policies
B. Review the security budget and resources
C. Participate in security training
D. Demonstrate good security practices
Answer: (SHOW ANSWER)
The correct answer is D because security culture is strongly influenced by leadership behavior. Senior management must set the tone from the top by consistently demonstrating good security practices, following policies, supporting security initiatives, and making risk-aware decisions. Employees are more likely to adopt secure behavior when they see executives and managers treating security as a business priority. Approving security policies is important, but approval alone does not create culture unless leaders also model expected behavior. Reviewing budget and resources supports the program, but it does not directly shape everyday security behavior. Participating in security training is positive and visible, but demonstrating good security practices on an ongoing basis has a broader cultural impact. In CISM governance, management commitment, accountability, communication, and example-setting are essential for embedding information security into the organization's values and operations. Therefore, leadership behavior is the most important factor in improving information security culture.
Reference: CISM Information Security Governance; security culture, tone at the top, senior management commitment, and organizational behavior principles.

NEW QUESTION: 375
Which of the following is BEST used to determine the maturity of an information security program?
A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics
Answer: (SHOW ANSWER)
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes.
Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.

References:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security- governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing- information-security

NEW QUESTION: 376
Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?
A. Effective security eliminates risk to the business.
B. Adopt a recognized framework with metrics.
C. Security is a business product and not a process.
D. Security supports and protects the business.
Answer: (SHOW ANSWER)
The message that security supports and protects the business is the most effective in obtaining senior management's commitment to information security management. This message emphasizes the value and benefits of security for the organization's strategic goals, mission, and vision. It also aligns security with the business needs and expectations, and demonstrates how security can enable and facilitate the business processes and functions. The other messages are not as effective because they either overstate the role of security (A), focus on technical aspects rather than business outcomes (B), or confuse the nature and purpose of security ©. References = CISM Review Manual 2022, page 23; CISM Item Development Guide 2022, page 9; CISM Information Security Governance Certified Practice Exam - CherCherTech

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 377
Which of the following is the PRIMARY reason for granting a security exception?
A. The risk is justified by the cost to the business.
B. The risk is justified by the benefit to security.
C. The risk is justified by the cost to security.
D. The risk is justified by the benefit to the business.
Answer: (SHOW ANSWER)

= A security exception is a formal authorization to deviate from a security policy, standard, or control, due to a valid business reason or requirement. The primary reason for granting a security exception is that the risk associated with the deviation is justified by the benefit to the business, such as increased efficiency, productivity, customer satisfaction, or competitive advantage. The security exception should be approved by the appropriate authority, such as the senior management or the risk committee, based on a risk assessment and a cost-benefit analysis. The security exception should also be documented, communicated, monitored, and reviewed periodically123. References =
* 1: CISM Review Manual 15th Edition, page 364
* 2: CISM Practice Quiz, question 1132
* 3: Security Policy Exception Management, section "Security Policy Exception Management Process"

NEW QUESTION: 378
After updating password standards, an information security manager is alerted by various application administrators that the applications they support are incapable of enforcing these standards. The information security manager's FIRST course of action should be to:
A. reevaluate the standards.
B. evaluate the cost of replacing the applications.
C. implement compensating controls.
D. determine the potential impact.
Answer: (SHOW ANSWER)

NEW QUESTION: 379
Which of the following BEST supports the adoption of effective information security practices throughout an organization?
A. Business continuity measures
B. A security-aware culture
C. The latest security technologies
D. Information security metrics
Answer: (SHOW ANSWER)
The correct answer is B because a security-aware culture encourages employees, managers, and stakeholders to consistently apply secure behaviors in daily operations. Effective security practices are adopted throughout an organization when people understand their responsibilities, recognize threats, and view security as part of business operations. Business continuity measures are important for resilience, but they do not broadly drive day-to-day adoption of security practices. The latest security technologies may improve technical protection, but technology alone cannot ensure people follow secure processes. Information security metrics help monitor and report performance, but they do not by themselves create behavioral adoption. CISM emphasizes that information security governance depends on culture, leadership, communication, awareness, and accountability. A security-aware culture supports compliance

with policies, timely reporting of incidents, protection of information assets, and consistent risk-based decision-making. Therefore, among the available choices, a security-aware culture best supports effective organization-wide adoption of information security practices.
Reference: CISM Information Security Governance; security culture, awareness, communication, and organizational adoption principles.

NEW QUESTION: 380

Which of the following is MOST helpful to identify whether information security policies have been followed?

Freecram.net

A. Detective controls
B. Corrective controls
C. Preventive controls
D. Directive controls
Answer: (SHOW ANSWER)

NEW QUESTION: 381

Which of the following should be done FIRST when developing an information security strategy?
A. Identify owners of information assets
B. Develop security policies and standards
C. Determine the desired state of information security
D. Establish an information security steering committee
Answer: C (LEAVE A REPLY)
The correct answer is C because developing an information security strategy requires defining the desired future state of information security in alignment with enterprise objectives, risk appetite, legal requirements, and business priorities. A strategy describes where the organization wants to go and how information security will support business goals. Identifying information asset owners is important for risk management and accountability, but it is not the first strategic activity.
Developing security policies and standards should occur after the strategic direction is understood, because policies and standards must support the desired state.
Establishing an information security steering committee is a strong governance practice, but the question asks what should be done first when developing the strategy itself. In CISM, security strategy should be business- aligned and should define target capabilities, priorities, governance expectations, and risk management direction. Determining the desired state allows the organization to compare current capabilities against future needs and build a roadmap. Therefore, determining the desired state of information security is the best first step.
Reference: CISM Information Security Governance; information security strategy, desired state, business alignment, governance roadmap, and strategic planning principles.

NEW QUESTION: 382

An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.
Answer: (SHOW ANSWER)
A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:
* It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.
* It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
* It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
* It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
* It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.
The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. References = 1: What is a Gap Analysis? | Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:
1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.
infosecinstitute.com+2 more

NEW QUESTION: 383

An organization is planning to outsource the execution of its disaster recovery activities. Which of the following would be MOST important to include in the outsourcing agreement?
A. Definition of when a disaster should be declared
B. Requirements for regularly testing backups
C. Recovery time objectives (RTOs)
D. The disaster recovery communication plan
Answer: (SHOW ANSWER)
The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on the business impact analysis (BIA) and the risk assessment, and they reflect the business continuity requirements and expectations of the organization. By including the RTOs in the outsourcing agreement, the organization can ensure that the service provider is aware of and committed to meeting the agreed service levels and minimizing the downtime and losses in the event of a disaster. The other options are not as important as the RTOs, although they may be relevant and useful to include in the outsourcing agreement depending on the scope and nature of the disaster recovery services. References = CISM Review Manual 15th Edition, page 2471; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1033

NEW QUESTION: 384
Network isolation techniques are immediately implemented after a security breach to:
A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.
Answer: (SHOW ANSWER)
Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. References = CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers & Explanations Database -
12 Month Subscription, Question ID: 1162

NEW QUESTION: 385

Which of the following is CRITICAL to ensure the appropriate stakeholder makes decisions during a cybersecurity incident?

A. Stakeholder plan

B. Escalation plan

C. Up-to-date risk register

D. Asset classification

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

During a cybersecurity incident, it is vital to ensure that the right people are involved and that decision- making occurs promptly.

A). Stakeholder plan: While identifying stakeholders is important, it does not outline decision-making during an incident.

B). Escalation plan: This is the BEST answer because it specifies how incidents are escalated to the appropriate level of authority, ensuring timely and effective decisions.

C). Up-to-date risk register: Although useful for understanding risks, it does not facilitate decision-making in real-time incidents.

D). Asset classification: This helps identify critical assets but does not address decision-making protocols during an incident.

Reference: CISM Job Practice Area 4 (Information Security Incident Management) highlights the importance of escalation procedures to manage incidents efficiently.

NEW QUESTION: 386

Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage

B. Communicating with internal and external parties

C. Minimizing negative impact to critical operations

D. Classifying incidents

Answer: C (LEAVE A REPLY)

The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents.

The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.

Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the

appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed.
However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION: 387
During which of the following development phases is it MOST challenging to implement security controls?
A. Post-implementation phase
B. Implementation phase
C. Development phase
D. Design phase
Answer: (SHOW ANSWER)
The development phase is the stage of the system development life cycle (SDLC) where the system requirements, design, architecture, and implementation are performed. The development phase is most challenging to implement security controls because it involves complex and dynamic processes that may not be well understood or documented. Security controls are essential for ensuring the confidentiality, integrity, and availability of the system and its data, as well as for complying with regulatory and contractual obligations. However, security controls may also introduce additional costs, risks, and constraints to the development process, such as: Increased complexity and overhead of testing, verification, validation, and maintenance Reduced flexibility and agility of changing requirements or design Increased dependency on external vendors or third parties for security services or products Increased vulnerability to errors, defects, or vulnerabilities in the code or configuration Increased difficulty in measuring and reporting on

security performance or effectiveness Therefore, implementing security controls in the development phase requires careful planning, coordination, communication, and collaboration among all stakeholders involved in the SDLC. It also requires a clear understanding of the security objectives, scope, criteria, standards, policies, procedures, roles, responsibilities, and resources for the system. Moreover, it requires a proactive approach to identifying and mitigating potential threats or risks that may affect the security of the system.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
System Development Life Cycle (SDLC)2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: https://store.isaca.org/s
/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 388
Which of the following is the BEST way for the organization to ensure server backups at a warm site are properly maintained and usable during a disaster?
A. Review the backup media storage facilities at the warm site
B. Have duplicate equipment available at the warm site
C. Use the equipment at the warm site facility to read the backups
D. Inspect the facility and inventory the backups on a quarterly basis
Answer: (SHOW ANSWER)
The best way to ensure that backups at a warm site are properly maintained and usable during a disaster is to use the equipment at the warm site facility to read the backups . CISM emphasizes that backup and recovery capabilities must be tested, not merely documented or inspected. Reading the backups using warm- site equipment validates both the backup media and compatibility with the recovery environment. Reviewing storage facilities or inventorying backup media confirms that backups exist and are stored appropriately, but it does not prove they can be restored. Having duplicate equipment available is useful, but it does not confirm that the backup data is readable or usable. The core issue is recoverability, and the only reliable way to validate recoverability is through practical testing. In business continuity and disaster recovery management, testing verifies whether recovery procedures, media, systems, and personnel can achieve required recovery objectives. Therefore, using warm-site equipment to read the backups provides the strongest assurance that backups will be usable when needed.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - backup testing and disaster recovery readiness ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 389
Which of the following is a prerequisite for formulating a business continuity plan (BCP)?
A. Recovery time objectives (RTOs) for the business processes

B. Process maps for production applications
C. System recovery procedures for alternate-site processing
D. Comprehensive property inventory
Answer: A (LEAVE A REPLY)
Recovery time objectives (RTOs) (A) are a prerequisite for developing a BCP because they define how quickly critical business processes must be restored. CISM clearly identifies the business impact analysis (BIA) and its outputs-such as RTOs-as foundational inputs to continuity planning. Recovery procedures (C) and process maps (B) are developed after recovery requirements are known. Property inventories (D) support asset management but are not central to BCP formulation.
References: ISACA CISM Review Manual (Program management-BCP and BIA); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 390
Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:
Freecram.net
A. a function of the likelihood and impact, should a threat exploit a vulnerability.
B. the magnitude of the impact, should a threat exploit a vulnerability.
C. a function of the cost and effectiveness of controls over a vulnerability.
D. the likelihood of a given threat attempting to exploit a vulnerability
Answer: (SHOW ANSWER)
= According to the CISM Manual1, risk is defined as the combination of the probability of an event and its consequence. Therefore, determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as a function of the likelihood and impact, should a threat exploit a vulnerability.
Likelihood is the probability or frequency of a threat occurring, while impact is the magnitude or severity of the harm or loss that would result from a threat exploiting a vulnerability. The higher the likelihood and impact, the higher the risk. The lower the likelihood and impact, the lower the risk.
The other options are not correct because they do not capture the full expression of risk. Option B only considers the impact, but not the likelihood, of a threat exploiting a vulnerability. Option C confuses the risk with the risk response, which is the action taken to reduce or mitigate the risk. Option D only considers the likelihood, but not the impact, of a threat attempting to exploit a vulnerability.
References = CISM Manual1, Chapter 2: Information Risk Management (IRM), Section 2.1: Risk Concepts2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 2

NEW QUESTION: 391
Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?

A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.
D. Provide security awareness training to board executives.
Answer: (SHOW ANSWER)
The best way to help ensure alignment of the information security program with organizational objectives is A: Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by:
Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators Allocating and prioritizing the resources and budget for information security initiatives and projects Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 392
Which of the following BEST enables an information security manager to demonstrate the effectiveness of the information security and risk program to senior management?
A. Audit reports
B. Updated risk assessments
C. Counts of information security incidents

D. Monthly metrics
Answer: (SHOW ANSWER)

NEW QUESTION: 393
The PRIMARY purpose of conducting a business impact analysis (BIA) is to determine the:
A. resources needed for business recovery.
B. scope of the incident response plan.
C. recovery time objective (RTO).
D. scope of the business continuity program.
Answer: (SHOW ANSWER)

NEW QUESTION: 394
An organization is selecting security metrics to measure security performance, and a firewall specialist suggests tracking the number of external attacks blocked by the firewalls. Which of the following is the GREATEST concern with using this metric?
A. The number of blocked external attacks is not representative of the true threat profile.
B. The number of blocked external attacks will vary by month, causing inconsistent graphs.
C. The number of blocked external attacks is an indicator of the organization's popularity.
D. The number of blocked external attacks over time does not explain the attackers' motivations.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Metrics should provide meaningful insights into the organization's risk exposure and security performance.
Evaluating this option:
A). The number of blocked external attacks is not representative of the true threat profile: This is the BEST answer because counting attacks blocked does not reveal the effectiveness of security controls or the real risk environment.
B). The number of blocked external attacks will vary by month, causing inconsistent graphs: While variability is a concern, it does not make the metric invalid.
C). The number of blocked external attacks is an indicator of the organization's popularity: This is true but irrelevant to assessing the effectiveness of security measures.
D). The number of blocked external attacks over time does not explain the attackers' motivations: Understanding motivations is useful but not directly tied to evaluating the firewall metric's effectiveness.
Reference: CISM Job Practice Area 2 (Risk Management) emphasizes the need for meaningful and risk-based metrics.

NEW QUESTION: 395
Which of the following provides an information security manager with the MOST accurate indication of the organization ' s ability to respond to a cyber attack?
A. Walk-through of the incident response plan

B. Black box penetration test
C. Simulated phishing exercise
D. Red team exercise
Answer: (SHOW ANSWER)
A red team exercise is a simulated cyber attack conducted by a group of ethical hackers or security experts (the red team) against an organization's network, systems, and staff (the blue team) to test the organization's ability to detect, respond, and recover from a real cyber attack. A red team exercise provides an information security manager with the most accurate indication of the organization's ability to respond to a cyber attack, because it mimics the tactics, techniques, and procedures of real threat actors, and challenges the organization' s security posture, incident response plan, and security awareness in a realistic and adversarial scenario12. A red team exercise can measure the following aspects of the organization's cyber attack response capability3:
The effectiveness and efficiency of the security controls and processes in preventing, detecting, and mitigating cyber attacks The readiness and performance of the incident response team and other stakeholders in following the incident response plan and procedures The communication and coordination among the internal and external parties involved in the incident response process The resilience and recovery of the critical assets and functions affected by the cyber attack The lessons learned and improvement opportunities identified from the cyber attack simulation The other options, such as a walk-through of the incident response plan, a black box penetration test, or a simulated phishing exercise, are not as accurate as a red team exercise in indicating the organization's ability to respond to a cyber attack, because they have the following limitations4 :
A walk-through of the incident response plan is a theoretical and hypothetical exercise that involves reviewing and discussing the incident response plan and procedures with the relevant stakeholders, without actually testing them in a live environment. A walk-through can help to familiarize the participants with the incident response roles and responsibilities, and to identify any gaps or inconsistencies in the plan, but it cannot measure the actual performance and effectiveness of the incident response process under a real cyber attack scenario.
A black box penetration test is a technical and targeted exercise that involves testing the security of a specific system or application, without any prior knowledge or access to its internal details or configuration. A black box penetration test can help to identify the vulnerabilities and weaknesses of the system or application, and to simulate the perspective and behavior of an external attacker, but it cannot test the security of the entire network or organization, or the response of the incident response team and other stakeholders to a cyber attack.
A simulated phishing exercise is a social engineering and awareness exercise that involves sending fake emails or messages to the organization's staff, to test their ability to recognize and report phishing attempts. A simulated phishing exercise can help to measure the level of security awareness and training of the staff, and to simulate one of the most common cyber attack vectors, but it cannot test the security of the network or systems, or the response of the incident response team and other stakeholders to a cyber attack.

References = 1: What is a Red Team Exercise? | Redscan 2: Red Team vs Blue Team: How They Differ and Why You Need Both | CISA 3: Red Team Exercises: What They Are and How to Run Them | Rapid7 4: What is a Walkthrough Test? | Definition and Examples | ISACA : Penetration Testing Types: Black Box, White Box, and Gray Box | CISA

NEW QUESTION: 396
Which of the following is the MOST important consideration when updating procedures for managing security devices?
A. Updates based on the organization's security framework
B. Notification to management of the procedural changes
C. Updates based on changes m risk technology and process
D. Review and approval of procedures by management
Answer: (SHOW ANSWER)
According to the CISM Manual, updating procedures for managing security devices should be based on changes in risk technology and process, not on the organization's security framework, notification to management of the procedural changes, or review and approval of procedures by management1. These are not the most important considerations when updating procedures for managing security devices, as they do not reflect the actual impact of the changes on the security posture of the organization.
The CISM Manual states that "procedures for managing security devices should be updated whenever there are significant changes in the risk technology or process that affect the security devices" (IR 8287A)1. For example, if a new security device is introduced or an existing one is replaced, its procedures should be updated accordingly. Similarly, if a new risk technology or process is implemented that affects how security devices are configured, monitored, or maintained, its procedures should be updated as well1.
The CISM Manual also provides guidance on how to update procedures for managing security devices in a systematic and consistent manner. It recommends using a change management process that involves identifying, analyzing, approving, implementing, and evaluating changes to security device procedures1. It also suggests using a change control board (CCB) that consists of representatives from different stakeholders who review and approve changes to security device procedures before they are implemented1.
References: 1: IR 8287A - Managing Security Devices | CSRC NIST

NEW QUESTION: 397
Which of the following BEST enables an organization to continuously assess the information security risk posture?
A. Degree of senior management support
B. Compliance with industry regulations
C. Key risk indicators (KRIs)
D. Periodic review of the risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 398
Which of the following should be done FIRST when developing a business continuity plan (BCP)?
A. Prioritize the critical processes.
B. Review current recovery policies.
C. Review existing cyber insurance coverage.
D. Define the organizational strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 399
Behavioral analytics tools are used PRIMARILY to manage risks within an organization by:
A. Preventing the exfiltration of sensitive data
B. Analyzing communications from external users for malware
C. Establishing security baselines on endpoints
D. Detecting anomalous user activities
Answer: (SHOW ANSWER)
The correct answer is D because behavioral analytics tools are primarily used to detect activities that deviate from normal user or entity behavior. These tools analyze patterns such as login times, access locations, data usage, application activity, privilege use, file access, and network behavior to identify anomalies that may indicate insider threats, compromised accounts, credential misuse, or advanced attacks. Preventing data exfiltration is normally associated with data loss prevention controls, although behavioral analytics may help detect suspicious activity related to exfiltration. Analyzing external communications for malware is more closely associated with email security gateways, web gateways, sandboxing, or malware detection tools. Establishing security baselines on endpoints is more related to configuration management or endpoint protection. In CISM risk management, behavioral analytics supports monitoring, detection, and risk reduction by identifying unusual activity that may require investigation. Since its primary value is identifying behavior that differs from expected patterns, detecting anomalous user activities is the best answer.
Reference: CISM Information Risk Management; user behavior analytics, monitoring controls, anomaly detection, insider threat, and risk detection principles.

NEW QUESTION: 400
Which of the following BEST enables the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption?
Freecram.net
A. Service level agreement (SLA)
B. Business continuity plan (BCP)
C. Disaster recovery plan (DRP)
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

The best option to enable the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption is B. Business continuity plan (BCP). This is because a BCP is a documented collection of procedures and information that guides the organization to prepare for, respond to, and recover from a disruption, such as a natural disaster, a cyberattack, or a pandemic. A BCP aims to ensure the continuity of the critical business functions and processes that support the delivery of products and services to the customers and stakeholders. A BCP also defines the roles, responsibilities, resources, and actions required to maintain the operational resilience of the organization in the face of a disruption.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.3, page 2141; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 6, page 3

NEW QUESTION: 401
An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?
A. Determine whether the organization can benefit from adopting the new standard.
B. Obtain legal counsel's opinion on the standard's applicability to regulations,
C. Perform a risk assessment on the new technology.
D. Review industry specialists' analyses of the new standard.
Answer: (SHOW ANSWER)
= The first step that the information security manager should recommend when learning of a new standard related to an emerging technology is to determine whether the organization can benefit from adopting the new standard. This involves evaluating the business objectives, needs, and requirements of the organization, as well as the potential advantages, disadvantages, and challenges of implementing the new technology and the new standard. The information security manager should also consider the alignment of the new standard with the organization's existing policies, procedures, and standards, as well as the impact of the new standard on the organization's information security governance, risk management, program, and incident management. By conducting a preliminary analysis of the feasibility, suitability, and desirability of the new standard, the information security manager can provide a sound basis for further decision making and planning.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Standards, page 391; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 43, page 412.

NEW QUESTION: 402
When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure:
A. forensic investigation software is loaded on the server.

B. the integrity of evidence is preserved.
C. the server is unplugged from power.
D. the incident is reported to senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 403
Which of the following should be done FIRST once a cybersecurity attack has been confirmed?
A. Isolate the affected system.
B. Notify senior management.
C. Power down the system.
D. Contact legal authorities.
Answer: (SHOW ANSWER)
Isolating the affected system is the first step in the incident response process, as it helps to contain the attack, prevent further damage, and preserve the evidence for analysis. Isolating the system can be done by disconnecting it from the network, blocking the malicious traffic, or applying quarantine rules.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.22; Cybersecurity Incident Response Exercise Guidance3

NEW QUESTION: 404
When evaluating vendors for sensitive data processing, which of the following should be the FIRST step to ensure the correct level of information security is provided?
A. Include information security clauses in the vendor contract.
B. Review third-party reports of potential vendors.
C. Develop metrics for vendor performance.
D. Include information security criteria as part of vendor selection.
Answer: (SHOW ANSWER)
The first step is to include information security criteria as part of vendor selection (D). CISM third-party risk management guidance stresses that security requirements must be defined before contracting or performance measurement. Contracts (A), reports (B), and metrics (C) are ineffective if the vendor was not selected based on the organization's security needs. Embedding security criteria early ensures only vendors capable of meeting required controls, compliance, and risk thresholds are considered.
References: ISACA CISM Review Manual (Governance-third-party risk management); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 405
Which of the following is the GREATEST value provided by a security information and event management (SIEM) system?
A. Maintaining a repository base of security policies
B. Measuring impact of exploits on business processes

C. Facilitating the monitoring of risk occurrences
D. Redirecting event logs to an alternate location for business continuity plan
Answer: (SHOW ANSWER)
A security information and event management (SIEM) system is a tool that collects, analyzes, and correlates security events from various sources, such as firewalls, intrusion detection systems, antivirus software, and other devices. A SIEM system can provide real-time alerts, dashboards, reports, and forensic analysis of security incidents. The greatest value of a SIEM system is that it can facilitate the monitoring of risk occurrences by identifying anomalies, trends, patterns, and indicators of compromise that may otherwise go unnoticed. A SIEM system can also help with incident response, compliance, and audit activities by providing evidence and documentation of security events.
References =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2291
ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2082 The greatest value provided by a Security Information and Event Management (SIEM) system is facilitating the monitoring of risk occurrences. SIEM systems collect, analyze and alert on security-related data from various sources such as firewall logs, intrusion detection/prevention systems, and system logs. This allows organizations to identify security threats in real-time and respond quickly, helping to mitigate potential harm to their systems and data.

NEW QUESTION: 406
What is the MOST important consideration for an organization operating in a highly regulated market when new regulatory requirements with high impact to the business need to be implemented?
A. Establishing compensating controls
B. Enforcing strong monitoring controls
C. Engaging an external audit
D. Conducting a gap analysis
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 407

A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?

A. Automated controls

B. Security policies

C. Guidelines

D. Standards

Answer: (SHOW ANSWER)

Standards are the most important thing to review, as they define the specific and mandatory requirements for setting up new user accounts, such as the naming conventions, access rights, password policies, and expiration dates. Standards help to ensure consistency, security, and compliance across the organization's information systems and users. If the standards are not followed, the organization may face increased risks of unauthorized access, data breaches, or audit failures.

References = CISM Review Manual 2022, page 341; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.32; CISM 2020: IT Security Policies; Information Security Policy, Standards, and Guidelines

NEW QUESTION: 408

In order to gain organization-wide support for an information security program, which of the following is MOST important to consider?

A. Maturity of the security policy

B. Clarity of security roles and responsibilities

C. Corporate culture

D. Corporate risk framework

Answer: (SHOW ANSWER)

Corporate culture is the most important factor to consider when trying to gain organization-wide support for an information security program because it reflects the values, beliefs, and behaviors of the organization and its members. Corporate culture influences how the organization perceives, prioritizes, and responds to information security risks and issues, and how it adopts and implements information security policies and practices. By understanding and aligning with the corporate culture, the information security manager can communicate the benefits and value of the information security program, and foster a positive and collaborative security culture across the organization.

References: The CISM Review Manual 2023 states that "corporate culture is the set of shared values, beliefs, and behaviors that characterize the organization and its members" and that "corporate culture affects how the organization views and manages information security risks and issues, and how it supports and implements information security policies and practices" (p. 81). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Corporate culture is the correct answer because it is the most important factor to consider when trying to gain organization-wide support for an information security program, as it reflects the values, beliefs, and behaviors of the organization and its members, and

influences how they perceive, prioritize, and respond to information security risks and issues, and how they adopt and implement information security policies and practices" (p. 23). Additionally, the article Building a Culture of Security from the ISACA Journal 2019 states that "corporate culture is the key factor that determines the success or failure of an information security program" and that "corporate culture can be either an enabler or a barrier for information security, depending on how well it aligns with the information security objectives, values, and practices of the organization" (p. 1)

NEW QUESTION: 409
Which of the following BEST enables an organization to evaluate the security posture of a cloud service?
A. Industry peer reviews
B. Service provider attestations
C. Penetration testing reports
D. Third-party audit reports
Answer: (SHOW ANSWER)
Third-party audit reports (D) provide the most reliable evaluation of a cloud provider's security posture because they offer independent assurance of control design and effectiveness. Peer reviews (A) and attestations (B) are less objective, while penetration test reports (C) focus narrowly on technical vulnerabilities. CISM emphasizes independent assurance mechanisms when assessing third-party security, particularly for cloud services.
References: ISACA CISM Review Manual (Governance-third-party assurance and cloud risk); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 410
The GREATEST challenge when attempting data recovery of a specific file during forensic analysis is when:
Freecram.net
A. the partition table on the disk has been deleted.
B. the tile has been overwritten.
C. all files in the directory have been deleted.
D. high-level disk formatting has been performed.
Answer: (SHOW ANSWER)
Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.
Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.
However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table,

the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. References = CISM Review Manual,
16th Edition, Chapter 5, Section 5.4.1.2

NEW QUESTION: 411
Which of the following is MOST important for a healthcare organization to address during the requirements gathering phase of AI development?
A. Algorithm selection challenges
B. Data privacy concerns
C. Inadequate computational resources
D. Data labeling inefficiencies
Answer: (SHOW ANSWER)
The most important consideration during the requirements gathering phase of AI development in a healthcare organization is data privacy concerns (B). From a CISM governance and risk management perspective, healthcare organizations handle highly sensitive personal and regulated data, such as protected health information (PHI), which is subject to strict privacy, confidentiality, and regulatory requirements. During requirements gathering, it is critical to ensure that legal, regulatory, and ethical obligations related to data use, retention, consent, access controls, and cross-border processing are fully understood and incorporated into system requirements.
Algorithm selection (A), computational resources (C), and data labeling efficiencies (D) are important technical and operational considerations, but they are secondary and should be addressed only after privacy requirements are clearly defined. CISM emphasizes that security and privacy must be built in by design, not retrofitted later in development. Failure to address privacy requirements early can result in regulatory noncompliance, reputational damage, and unacceptable risk exposure.
In healthcare, governance-driven requirements-especially privacy, data minimization, and lawful processing-must guide AI system design to ensure alignment with organizational risk appetite and compliance obligations.
References:
ISACA CISM Review Manual, Information Security Governance - privacy, regulatory compliance, and emerging technology risk ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 412
Which of the following would be MOST helpful to identify worst-case disruption scenarios?
A. Business impact analysis (BIA)
B. Business process analysis
C. SWOT analysis
D. Cast-benefit analysis
Answer: (SHOW ANSWER)

A business impact analysis (BIA) is the process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization in the event of a disaster or crisis. A BIA also helps to identify the worst-case disruption scenarios, which are the scenarios that would cause the most severe impact to the organization in terms of financial, operational, reputational, or legal consequences. By conducting a BIA, the organization can assess the likelihood and impact of various disruption scenarios, and plan accordingly to mitigate the risks and ensure business continuity and resilience. References = CISM Review Manual 15th Edition, page 181, page 183.

NEW QUESTION: 413
Which of the following roles has the PRIMARY responsibility to ensure the operating effectiveness of IT controls?
A. Risk owner
B. Control tester
C. IT compliance leader
D. Information security manager
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition1, the information security manager is responsible for ensuring that the information security program supports the organization's objectives and aligns with applicable laws and regulations. The information security manager is also responsible for overseeing the implementation and maintenance of effective IT controls, as well as monitoring and reporting on their performance.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 1, page 10.

NEW QUESTION: 414
Which of the following BEST enables staff acceptance of information security policies?
A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program
D. Adequate security funding
Answer: A (LEAVE A REPLY)
= Strong senior management support is the best factor to enable staff acceptance of information security policies, as it demonstrates the commitment and leadership of the organization's top executives in promoting and enforcing a security culture. Senior management support can also help ensure that the information security policies are aligned with the business goals and values, communicated effectively to all levels of the organization, and integrated into the performance evaluation and reward systems. Senior management support can also help overcome any resistance or challenges from other stakeholders, such as business units, customers, or regulators123. References =
1: CISM Review Manual 15th Edition, page 26-274

2: CISM Practice Quiz, question 1102
3: Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, page 5-6

NEW QUESTION: 415
An online bank identifies a successful network attack in progress. The bank should FIRST:
A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (PII) is compromised.
D. shut down the entire network.
Answer: (SHOW ANSWER)
The online bank should first isolate the affected network segment, as this is the most effective way to contain the attack and prevent it from spreading to other parts of the network or compromising more data or systems.
Isolating the affected network segment also helps to preserve the evidence and facilitate the investigation and recovery process. Reporting the root cause to the board of directors, assessing whether personally identifiable information (PII) is compromised, and shutting down the entire network are not the first actions that the online bank should take, as they may not be feasible or appropriate at the time of the attack, and may cause more disruption, confusion, or damage to the business operations and reputation. References = CISM Review Manual 2023, page 1641; CISM Review Questions, Answers & Explanations Manual 2023, page 362; ISACA CISM - iSecPrep, page 213

NEW QUESTION: 416
While conducting a test of a business continuity plan (BCP), which of the following is the MOST important consideration?
A. The test is scheduled to reduce operational impact.
B. The test involves IT members in the test process.
C. The test addresses the critical components.
D. The test simulates actual prime-time processing conditions.
Answer: (SHOW ANSWER)
The test addresses the critical components is the most important consideration while conducting a test of a business continuity plan (BCP), as it ensures that the test covers the essential functions, processes, and resources that are required to maintain or resume the organization's operations in the event of a disruption.
The test should also verify that the recovery objectives, such as recovery time objective (RTO) and recovery point objective (RPO), are met. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1; CISSP Exam Cram: Business Continuity and Disaster Recovery Planning1, page 5, section Testing the Plan.

NEW QUESTION: 417

Which of the following is the BEST reason to implement an information security architecture?
A. Fast-track the deployment of information security components.
B. Facilitate consistent implementation of security requirements.
C. Serve as a post-deployment information security road map.
D. Assess the cost-effectiveness of the integration.
Answer: (SHOW ANSWER)

NEW QUESTION: 418
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?
A. Employee training on ransomware
B. A properly tested offline backup system
C. A continual server replication process
D. A properly configured firewall
Answer: B (LEAVE A REPLY)
The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures.
Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware.
However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable.
A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 419
As part of a risk assessment, a security control was discovered to be inadequate. When assigning a risk owner, which of the following attributes is MOST important to consider?
A. The risk owner is able to reassess the risk following remediation.

B. The risk owner has the authority to take action on the risk.
C. The risk owner is able to make timely updates to the risk register.
D. The risk owner also owns the associated control that failed.
Answer: (SHOW ANSWER)
The most important attribute when assigning a risk owner is that the risk owner has the authority to take action on the risk (B). In CISM, risk ownership is fundamentally about accountability and decision-making authority. The risk owner must be empowered to decide on risk treatment options-such as mitigation, transfer, acceptance, or avoidance-and to allocate resources or approve changes necessary to address the risk.
While reassessing risk after remediation (A) and updating the risk register (C) are important responsibilities, they are administrative and follow-on activities that do not, by themselves, ensure effective risk management.
Ownership of the failed control (D) is not required; in fact, CISM distinguishes between risk ownership (business accountability) and control ownership (operational responsibility). The risk owner is typically a business role accountable for the impact of the risk, not necessarily the individual responsible for implementing or operating the control.
CISM guidance consistently stresses that risk owners must have sufficient authority, accountability, and understanding of business impact to make informed decisions aligned with the organization's risk appetite.
Without authority, risk ownership becomes ineffective and purely symbolic.
References:
ISACA CISM Review Manual, Information Risk Management - risk ownership, accountability, and risk response ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

NEW QUESTION: 420
Which of the following BEST indicates ongoing senior management commitment to the organization's information security strategy?
Freecram.net
A. Established key performance indicators
B. A comprehensive security awareness training program
C. An efficient incident response program
D. Adequate funding for the information security program
Answer: (SHOW ANSWER)
The correct answer is D because adequate funding demonstrates that senior management is actively supporting the information security strategy with the resources required for implementation and sustainability.
A strategy cannot be effective unless it is backed by budget, staffing, tools, training, governance support, and operational capability. Key performance indicators help measure progress, but they do not by themselves prove management commitment. A comprehensive awareness program is valuable, but it may exist without broad strategic support. An efficient incident response program is important, but it represents one part of the overall security program. In CISM, senior management commitment is reflected through sponsorship, direction, resource allocation,

accountability, and continuous support. Funding is especially important because it enables security initiatives to be executed and maintained over time. Without adequate resources, even a well-designed strategy may fail. Therefore, adequate funding for the information security program is the best indicator of ongoing senior management commitment.
Reference: CISM Information Security Governance; senior management commitment, resource allocation, strategy execution, and program sponsorship principles.

NEW QUESTION: 421
An incident response plan is being developed for servers hosting sensitive information. In the event of a breach, who should make the decision to shut down the system?
A. Service owner
B. Information security manager
C. Operations manager
D. Incident response team
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 422
What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?
A. Developing a dashboard for communicating the metrics
B. Agreeing on baseline values for the metrics
C. Benchmarking the expected value of the metrics against industry standards
D. Aligning the metrics with the organizational culture
Answer: (SHOW ANSWER)
The most important consideration when establishing metrics for reporting to the information security strategy committee is D. Aligning the metrics with the organizational culture. This is because the metrics should reflect the values, beliefs, and behaviors of the organization and its stakeholders, and support the achievement of the strategic objectives and goals. The metrics should also be relevant, meaningful, and understandable for the intended audience, and provide clear and actionable information for decision making. The metrics should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.

References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 5, page 3

NEW QUESTION: 423
Which of the following is the BEST way to determine the effectiveness of an incident response plan?
A. Reviewing previous audit reports
B. Conducting a tabletop exercise
C. Benchmarking the plan against best practices
D. Performing a penetration test
Answer: (SHOW ANSWER)
A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

NEW QUESTION: 424
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?
A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes
Answer: (SHOW ANSWER)
Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations.
References = CISM Review Manual 2023, page 291; CISM Review Questions, Answers &

Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

NEW QUESTION: 425
Risk treatment options should PRIMARILY focus on:
A. The criticality of impacted assets
B. Reducing risk to an acceptable level
C. High- and medium-rated risks
D. Inherent and residual risks
Answer: (SHOW ANSWER)
The correct answer is B because the purpose of risk treatment is to bring risk within the organization's acceptable level, based on risk appetite and risk tolerance. Risk treatment may involve mitigating, avoiding, transferring, or accepting risk. The objective is not simply to focus on inherent and residual risk as concepts, but to select and apply treatment options that reduce or manage risk to a level approved by the organization.
Asset criticality is an important input because more critical assets may require stronger controls, but it is not the primary purpose of treatment. High- and medium-rated risks often receive priority, but risk treatment should still be based on business impact, likelihood, cost, risk appetite, and treatment effectiveness. Inherent and residual risk must be understood, but they describe risk before and after controls rather than the main focus of selecting treatment. CISM risk management principles emphasize that management must choose treatment options that align risk with business objectives and acceptable risk levels.
Reference: CISM Information Risk Management; risk treatment, risk appetite, residual risk, and risk response principles.

NEW QUESTION: 426
A technical vulnerability assessment on a personnel information management server should be performed when:
A. the data owner leaves the organization unexpectedly.
B. changes are made to the system configuration.
C. the number of unauthorized access attempts increases.
D. an unexpected server outage has occurred.
Answer: (SHOW ANSWER)
A technical vulnerability assessment is a process of identifying and evaluating the weaknesses and risks associated with a specific system, component, or network. A technical vulnerability assessment can help to determine the potential impact and likelihood of a security breach, as well as the appropriate measures to prevent or mitigate it. A technical vulnerability assessment should be performed on a personnel information management server whenever there is an increase in the number of unauthorized access attempts to the server, as this indicates that the server may have been compromised or targeted by an attacker12. Therefore, option C is the correct answer.
References = CISM Review Manual (Digital Version), Chapter 5: Information Security Program

Management CISM Review Manual (Print Version), Chapter 5: Information Security Program Management

NEW QUESTION: 427
Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?
A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.
D. Identify recovery time objectives (RTOs).
Answer: (SHOW ANSWER)
= Developing the test plan is the task that should be performed once a disaster recovery plan (DRP) has been developed. The test plan is a document that describes the objectives, scope, methods, and procedures for testing the DRP. The test plan should also define the roles and responsibilities of the test team, the test scenarios and criteria, the test schedule and resources, and the test reporting and evaluation. The purpose of testing the DRP is to verify its effectiveness, identify any gaps or weaknesses, and improve its reliability and usability. Testing the DRP also helps to increase the awareness and readiness of the staff and stakeholders involved in the disaster recovery process. Analyzing the business impact, defining response team roles, and identifying recovery time objectives (RTOs) are all tasks that should be performed before developing the DRP, not after. These tasks are part of the business continuity planning (BCP) process, which aims to identify the critical business functions and assets, assess the potential threats and impacts, and determine the recovery strategies and requirements. The DRP is a subset of the BCP that focuses on restoring the IT systems and services after a disaster. Therefore, the DRP should be based on the results of the BCP process, and tested after it has been developed. References = CISM Review Manual 2023, page 218 1; CISM Practice Quiz 2

NEW QUESTION: 428
What is the role of the information security manager in finalizing contract negotiations with service providers?
A. To perform a risk analysis on the outsourcing process
B. To obtain a security standard certification from the provider
C. To update security standards for the outsourced process
D. To ensure that clauses for periodic audits are included
Answer: (SHOW ANSWER)
The role of the information security manager in finalizing contract negotiations with service providers is to ensure that the outsourcing process is aligned with the organization's information security policies, standards, and objectives. One of the key aspects of this process is to perform a risk analysis on the outsourcing process, which involves identifying, assessing, and mitigating the potential threats and vulnerabilities that may arise from outsourcing activities. A risk analysis can help the information security manager to determine the appropriate level of security controls and

requirements for the outsourced process, as well as to monitor and evaluate its performance and compliance. A risk analysis can also help to avoid or minimize legal, financial, reputational, or operational risks associated with outsourcing1. References = CISM Review Manual (Digital Version), Chapter 6: Information Security Program Management CISM Review Manual (Print Version), Chapter 6: Information Security Program Management

NEW QUESTION: 429
Which of the following would be the BEST way to reduce the risk of disruption resulting from an emergency system change?
A. Confirm the change implementation is scheduled.
B. Verify the change request has been approved.
C. Confirm rollback plans are in place.
D. Notify users affected by the change.
Answer: C (LEAVE A REPLY)
The best way to reduce the risk of disruption from an emergency system change is to confirm rollback plans are in place. According to the CISM Review Manual, having an effective rollback (or backout) plan ensures that if the emergency change causes unexpected issues, the organization can quickly revert to a known, stable state. This minimizes downtime and impact to business operations. Approval and communication are important, but only a rollback plan directly addresses risk reduction during unexpected disruptions.
Reference:ISACA CISM Review Manual, 16th Edition, Page 210, "Change Management - Rollback Planning".

NEW QUESTION: 430
Which of the following is the GREATEST challenge when developing key risk indicators (KRIs)?
A. Limiting the number of KRIs
B. Comprehensively reporting on KRIs
C. Aggregating common KRIs
D. Linking KRIs to specific risks
Answer: (SHOW ANSWER)
The biggest challenge is linking KRIs to specific risks to ensure that they accurately measure and signal potential exposures. If KRIs aren't directly connected to real risks, they won't effectively support risk management efforts.
"A key challenge in developing KRIs is ensuring that they are directly linked to specific risks to provide meaningful and actionable insights."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Key Risk Indicators (KRIs)* ISACA's practice questions highlight the importance of clear linkage for effective risk measurement.

NEW QUESTION: 431

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

A. Integrating the risk assessment into the internal audit program

B. Having the information security manager participate on the project steering committees

C. Training project managers on risk assessment

D. Applying global security standards to the IT projects

Answer: (SHOW ANSWER)

NEW QUESTION: 432

The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents.

B. identify vulnerabilities.

C. identify control improvements.

D. identify the root cause.

Answer: (SHOW ANSWER)

= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.

Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.

Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re- evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.

Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.

Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. References = ISACA CISM: PRIMARY goal of a post-incident review should be to?

CISM Exam Overview - Vinsys

CISM Review Manual, Chapter 4, page 176
CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

NEW QUESTION: 433
An organization is strategizing on how to improve security awareness. Which of the following is MOST important to consider when developing this strategy?
A. Organizational maturity
B. Cost to implement
C. Organizational culture
D. Technical solutions for delivery
Answer: (SHOW ANSWER)
Organizational culture (C) is the most important factor when developing a security awareness strategy because culture determines how messages are received, accepted, and acted upon. CISM emphasizes that awareness programs must be tailored to the organization's values, behaviors, leadership tone, and risk mindset. Even well-funded programs or advanced delivery platforms will fail if they do not align with how employees think and work. Organizational maturity (A) and cost (B) influence scope and pacing, while technical delivery methods (D) are implementation details. A culture-aware approach ensures that security awareness drives behavioral change, which is the ultimate goal of awareness initiatives.
References: ISACA CISM Review Manual (Program management-security culture, awareness and training); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 434
A health care organization has been informed of a breach at a third-party vendor. Which of the following should the organization's information security manager do FIRST?
A. Notify relevant regulatory bodies
B. Review the relevant contract clauses
C. Assess the impact
D. Notify senior management
Answer: (SHOW ANSWER)
The correct answer is C because the first step after being informed of a third-party vendor breach is to assess the impact on the organization. The information security manager must determine whether organizational data, patient information, regulated records, systems, services, or business processes were affected. This assessment helps determine incident severity, legal notification obligations, regulatory reporting requirements, contractual rights, business impact, and required containment actions. Notifying regulatory bodies may be required in a health care context, but notification should be based on confirmed facts such as affected data types, number of individuals impacted, jurisdiction, and reporting thresholds. Reviewing contract clauses is important to understand vendor obligations, breach notification timelines, audit rights, and liability, but the organization first needs to understand the impact. Notifying senior management may be necessary for significant incidents, but meaningful notification depends on initial impact

assessment. CISM incident management and third-party risk principles emphasize timely assessment, classification, escalation, and response. Therefore, assessing impact is the correct first action.
Reference: CISM Information Security Incident Management; third-party breach response, impact assessment, health care data protection, and incident escalation principles.

NEW QUESTION: 435
Which of the following BEST indicates senior management support for an information security program?
A. Top-down communication
B. Regular security awareness training
C. Steering committee involvement
D. Participation in a certification program
Answer: (SHOW ANSWER)
The correct answer is C because active involvement in an information security steering committee demonstrates senior management's ongoing participation in governance, prioritization, decision-making, and oversight. Senior management support is not shown only by words or occasional communication; it is demonstrated through active engagement, resource allocation, risk decisions, and accountability. Top-down communication is useful and may show support, but it is less meaningful than direct participation in a governance body. Regular security awareness training is important for employees, but it does not necessarily prove senior management support. Participation in a certification program may improve professional skills or demonstrate individual commitment, but it is not the best indicator of organizational leadership support. In CISM, information security governance requires senior management direction and oversight to ensure that security objectives align with business objectives. A steering committee provides a formal mechanism for that oversight and involvement. Therefore, steering committee involvement is the best indicator of senior management support.
Reference: CISM Information Security Governance; senior management commitment, steering committee oversight, and governance accountability principles.

NEW QUESTION: 436
Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?
A. Require remote wipe capabilities for devices.
B. Conduct security awareness training.
C. Review and update existing security policies.
D. Enforce passwords and data encryption on the devices.
Answer: (SHOW ANSWER)
The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation's security

program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be reviewed and updated regularly to reflect changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities, as well as new opportunities and benefits, for the organiza-tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:
*The scope, purpose, and ownership of company-owned mobile devices
*The acceptable and unacceptable use of company-owned mobile devices
*The security standards and best practices for company-owned mobile devices
*The roles and responsibilities of users, managers, IT staff, and vendors regarding compa-ny-owned mobile devices
*The procedures for provisioning, managing, monitoring, and decommissioning company-owned mobile devices
*The incident response and reporting process for company-owned mobile devices By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com-promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices. References:
1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is
& How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 437

Which of the following should be the PRIMARY objective for creating a culture of security within an organization?
A. To obtain resources for information security initiatives
B. To prioritize security within the organization
C. To reduce risk to acceptable levels
D. To demonstrate control effectiveness to senior management
Answer: C (LEAVE A REPLY)
The primary objective of creating a security culture is to reduce risk to acceptable levels (C) by influencing employee behavior and decision-making. CISM stresses that culture is a means to an end-not the end itself.
Prioritization (B), resource acquisition (A), and reporting (D) are outcomes or enablers, but the ultimate purpose is effective risk reduction aligned with business objectives. A strong security culture helps prevent incidents, improves compliance, and strengthens resilience through consistent, risk-aware behavior at all levels of the organization.
References: ISACA CISM Review Manual (Program management-security culture and behavior); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 438
How would the information security program BEST support the adoption of emerging technologies?
A. Conducting a control assessment
B. Developing an emerging technology roadmap
C. Providing effective risk governance
D. Developing an acceptable use policy
Answer: (SHOW ANSWER)
An emerging technology roadmap is a strategic plan that identifies the potential benefits, risks, and challenges of adopting new technologies in alignment with the organization's goals and objectives. It also defines the roles and responsibilities, processes, and controls for managing the technology lifecycle, from evaluation to implementation to maintenance. An emerging technology roadmap can help the information security program support the adoption of emerging technologies by ensuring that security requirements are considered and addressed at every stage, and that the technologies are aligned with the organization's risk appetite and compliance obligations.
References = CISM Review Manual, 15th Edition, page 97; Privacy, Security and Bias in Emerging Technologies; The Impact of Emerging Technology on the Future of Cybersecurity

NEW QUESTION: 439
The MOST effective tools for responding to new and advanced attacks are those that detect attacks based on:
A. penetration testing.
B. data packet analysis.

C. behavior analysis.
D. signature analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 440
Which of the following is the BEST way to compete for funding for an information security program in an organization with limited resources?
Freecram.net
A. Demonstrate that the program enables business activities
B. Report key performance indicator trends
C. Demonstrate the effectiveness of business continuity plans
D. Provide evidence of increased security events at peer organizations
Answer: (SHOW ANSWER)
The correct answer is A because information security programs compete more effectively for limited funding when they demonstrate clear business value. Senior management is more likely to fund initiatives that enable business activities, protect revenue, support strategic objectives, reduce unacceptable risk, maintain customer trust, and meet regulatory obligations. Reporting KPI trends may support the funding request, but metrics alone may not show why the program matters to business outcomes. Demonstrating business continuity plan effectiveness is useful, but it is only one part of resilience and does not justify the entire information security program. Evidence of increased security events at peer organizations can help show threat relevance, but external events do not necessarily prove the organization's business need. CISM governance emphasizes value delivery, business alignment, and risk-informed investment decisions. In resource-constrained environments, security should be positioned as a business enabler rather than simply a cost center. Therefore, demonstrating that the program enables business activities is the strongest approach.
Reference: CISM Information Security Governance; business alignment, value delivery, security investment, and senior management funding principles.

NEW QUESTION: 441
In a business proposal, a potential vendor promotes being certified for international security standards as a measure of its security capability.
Before relying on this certification, it is MOST important that the information security manager confirms that the:
A. current international standard was used to assess security processes.
B. certification will remain current through the life of the contract.
C. certification scope is relevant to the service being offered.
D. certification can be extended to cover the client's business.
Answer: (SHOW ANSWER)
Before relying on a vendor's certification for international security standards, such as ISO/IEC 27001, it is most important that the information security manager confirms that the certification scope is relevant to the service being offered. The certification scope defines the boundaries and

applicability of the information security management system (ISMS) that the vendor has implemented and audited. The scope should cover the processes, activities, assets, and locations that are involved in delivering the service to the client. If the scope is too narrow, too broad, or not aligned with the service, the certification may not provide sufficient assurance of the vendor's security capability and performance.

The current international standard was used to assess security processes (A) is an important factor, but not the most important one. The information security manager should verify that the vendor's certification is based on the latest version of the standard, which reflects the current best practices and requirements for information security. However, the standard itself is generic and adaptable, and does not prescribe specific security controls or solutions. Therefore, the certification does not guarantee that the vendor has implemented the most appropriate or effective security processes for the service being offered.

The certification will remain current through the life of the contract (B) is also an important factor, but not the most important one. The information security manager should ensure that the vendor's certification is valid and up to date, and that the vendor maintains its compliance with the standard throughout the contract period.

However, the certification is not a one-time event, but a continuous process that requires periodic surveillance audits and recertification every three years. Therefore, the certification does not ensure that the vendor's security capability and performance will remain consistent or satisfactory for the duration of the contract.

The certification can be extended to cover the client's business (D) is not a relevant factor, as the certification is specific to the vendor's ISMS and does not apply to the client's business. The information security manager should not rely on the vendor's certification to substitute or supplement the client's own security policies, standards, or controls. The information security manager should conduct a due diligence and risk assessment of the vendor, and establish a clear and comprehensive service level agreement (SLA) that defines the security roles, responsibilities, expectations, and metrics for both parties.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, page 142-1431

NEW QUESTION: 442

Which of the following is the MOST important factor in successfully implementing Zero Trust?

A. Preferring networks that have undergone penetration testing

B. Focusing on logging and monitoring of user behavior

C. Authenticating and authorizing strategic points of the architecture

D. Understanding each component of the network

Answer: (SHOW ANSWER)

Zero Trust requires granular authentication and authorization at every critical juncture. It assumes no implicit trust within the network and enforces strict access control.

"Zero Trust is based on continuous authentication and authorization at all strategic control points."

- CISM Review Manual 15th Edition, Chapter 3: Security Architecture, Section: Zero Trust Principles*

NEW QUESTION: 443
A new information security reporting requirement will soon become effective. Which of the following should be the information security manager's FIRST action?
A. Conduct a cost-benefit analysis related to noncompliance with the new requirement.
B. Perform a gap assessment against the new requirement.
C. Investigate to determine whether the new requirement applies to the business.
D. Inform senior management of the new requirement.
Answer: (SHOW ANSWER)
Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily.
"The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Compliance*

NEW QUESTION: 444
Which of the following would BEST justify continued investment in an information security program?
A. Reduction in residual risk
B. Security framework alignment
C. Speed of implementation
D. Industry peer benchmarking
Answer: A (LEAVE A REPLY)
Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. References = CISM Review Manual, 16th Edition, page 431; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 622 Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

NEW QUESTION: 445
Which of the following is MOST effective for real-time identification and mitigation of unauthorized access attempts in a Zero Trust Architecture?
A. Implementing continuous authentication based on behavioral analytics
B. Deploying network intrusion detection systems at the gateway
C. Conducting periodic vulnerability scans to reduce exploitable vulnerabilities
D. Enforcing strict password reuse and complexity policies for users
Answer: (SHOW ANSWER)
The correct answer is A because continuous authentication based on behavioral analytics is most consistent with the Zero Trust principle of "never trust, always verify." In a Zero Trust environment, access should be continuously evaluated based on identity, device posture, context, behavior, and risk signals. Behavioral analytics can identify suspicious deviations such as unusual login times, abnormal data access, impossible travel, unexpected privilege use, or atypical application activity. This allows immediate mitigation through step-up authentication, session termination, access restriction, or alert escalation. A gateway IDS is helpful for network monitoring but does not provide continuous identity-based access enforcement. Vulnerability scanning is important but periodic and preventive, not a real-time access mitigation mechanism. Password complexity and reuse policies are useful baseline controls but cannot detect unauthorized behavior during an active session. CISM principles emphasize risk-based, effective control selection. For real-time Zero Trust access protection, continuous authentication with behavioral analytics is the best answer.
Reference: CISM Information Security Program Development and Management; Zero Trust, identity assurance, behavioral analytics, and real-time access mitigation principles.

NEW QUESTION: 446
Which of the following would be MOST important to include in a proposal justifying investments for an organization's information security program?
A. Vulnerability scan results
B. Competitor benchmark analysis
C. Previous security budget
D. Business requirements
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Justifying investments in information security requires aligning proposals with business objectives to gain management approval.
A). Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.
B). Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.
C). Previous security budget: Historical data may provide context but does not justify future needs.

D). Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders. Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

NEW QUESTION: 447
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?
A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule
Answer: (SHOW ANSWER)
The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

NEW QUESTION: 448
The PRIMARY advantage of involving end users in continuity planning is that they:
A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.
Answer: (SHOW ANSWER)
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and

resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION: 449
Of the following, who is BEST suited to own the risk discovered in an application?
A. Senior management
B. Information security manager
C. Control owner
D. System owner
Answer: (SHOW ANSWER)

NEW QUESTION: 450
What is the PRIMARY role of the information security program?
A. To perform periodic risk assessments and business impact analyses (BIAs)
B. To provide guidance in managing organizational security risk
C. To approve information security requirements related to the business
D. To educate stakeholders regarding information security requirements
Answer: (SHOW ANSWER)
The primary role of the information security program is to provide guidance in managing organizational security risk (B). In CISM, the security program translates governance direction, policies, and risk appetite into coordinated activities, controls, and practices that enable the organization to manage risk consistently and effectively. Performing risk assessments and BIAs (A) are important activities but are not the program's primary purpose. Approving security requirements (C) is typically a management or governance responsibility, while education and awareness (D) are supporting components of the program. CISM emphasizes that the security program acts as the mechanism for operationalizing risk management, ensuring alignment with business objectives and continuous improvement of the security posture.
References: ISACA CISM Review Manual (Program development and management-program purpose and scope); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 451
Which of the following should occur FIRST in the process of managing security risk associated with the transfer of data from unsupported legacy systems to supported systems?
A. Perform security testing on legacy systems
B. Identify all information assets in the legacy environment
C. Assign owners to be responsible for the transfer of each asset
D. Conduct a business impact analysis (BIA)
Answer: (SHOW ANSWER)
The first step should be to identify all information assets in the legacy environment . Managing security risk during data transfer requires understanding what data and information assets exist

before evaluating impact, assigning ownership, testing, or selecting controls. CISM risk management emphasizes that asset identification is foundational because organizations cannot protect, classify, transfer, or assign accountability for assets they do not know exist. A business impact analysis may help prioritize critical processes and recovery requirements, but it does not replace the need to identify the data assets being transferred. Security testing of legacy systems may be useful later, especially if the systems remain operational during migration, but it is not the first step. Assigning owners is necessary, but ownership can only be accurately assigned after assets are identified. Unsupported legacy systems often contain undocumented data, obsolete interfaces, and unknown dependencies. Therefore, the first risk management activity must be creating an accurate inventory of information assets in the legacy environment.
References:
ISACA CISM Review Manual , Information Risk Management - asset identification, classification, and risk assessment ISACA CISM Exam Content Outline , Domain 1: Information Risk Management

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 452
Which of the following is MOST important when conducting a forensic investigation?
A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody
Answer: (SHOW ANSWER)
Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence.
References = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

NEW QUESTION: 453
An organization's automated security monitoring tool generates an excessively large amount of falsq positives. Which of the following is the BEST method to optimize the monitoring process?
A. Report only critical alerts.
B. Change reporting thresholds.
C. Reconfigure log recording.
D. Monitor incidents in a specific time frame.
Answer: (SHOW ANSWER)
Changing reporting thresholds is the best method to optimize the monitoring process when the automated security monitoring tool generates an excessively large amount of false positives. Changing reporting thresholds means adjusting the criteria or parameters that trigger the alerts, such as the severity level, the frequency, the source, or the destination of the events. Changing reporting thresholds can help to reduce the number of false positives, filter out the irrelevant or benign events, and focus on the most critical and suspicious events that require further investigation or response.
References = Cybersecurity tool sprawl leading to burnout, false positives: report, Security tools' effectiveness hampered by false positives

NEW QUESTION: 454
Results from which of the following would BEST provide an understanding of the effectiveness of an organization's information security program?
A. Security spot checks
B. Internal audits
C. Enterprise risk assessments
D. Control self-assessments (CSAs)
Answer: (SHOW ANSWER)
Control self-assessments (CSAs) (D) best provide an understanding of the effectiveness of an organization's information security program because they focus specifically on whether security controls are operating as intended on an ongoing basis. In CISM, program effectiveness is measured not only by design adequacy, but by consistent execution and performance of controls across the organization.
CSAs enable control owners and business stakeholders to evaluate control implementation, identify weaknesses, and report effectiveness in a structured and repeatable manner. This provides management with broad, timely, and actionable insight into how well the security program is functioning day to day. Internal audits (B) offer independent assurance but are typically periodic and retrospective. Enterprise risk assessments (C) focus on identifying and prioritizing risks, not on validating control performance. Security spot checks (A) are limited in scope and do not provide a comprehensive program view.

CISM emphasizes that effective security programs rely on continuous monitoring and self-assessment mechanisms to demonstrate control effectiveness, support improvement, and inform governance reporting.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - monitoring, measurement, and control effectiveness ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 455
An information security manager learns that a risk owner has approved exceptions to replace key controls with weaker compensating controls to improve process efficiency. Which of the following should be the GREATEST concern?
A. Risk levels may be elevated beyond acceptable limits.
B. Security audits may report more high-risk findings.
C. The compensating controls may not be cost efficient.
D. Noncompliance with industry best practices may result.
Answer: (SHOW ANSWER)
Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

NEW QUESTION: 456
What is the PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes?
A. Security incident reporting procedures are followed.
B. Security staff turnover is reduced.
C. Information assets are classified appropriately.
D. Access is granted based on task requirements.
Answer: (SHOW ANSWER)
The PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes is that access is granted based on task requirements. This means that the organization can ensure that the employees have the appropriate level and scope of access to the information assets and systems that they need to perform their duties, and that the access is granted, reviewed, and revoked in accordance with the security policies and standards. This can help to reduce the risk of unauthorized access,

misuse, or leakage of information, as well as to comply with the principle of least privilege and the segregation of duties12. Security incident reporting procedures are followed (A) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Security incident reporting procedures are the steps and guidelines that the employees should follow when they detect, report, or respond to a security incident.
Aligning the information security program requirements with the employment and staffing processes can help to ensure that the employees are aware of and trained on the security incident reporting procedures, and that they are enforced and monitored by the management. This can help to improve the effectiveness and efficiency of the incident response process, as well as to comply with the legal and contractual obligations12.
Security staff turnover is reduced (B) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit.
Security staff turnover is the rate at which the security personnel leave or join the organization. Aligning the information security program requirements with the employment and staffing processes can help to reduce the security staff turnover by ensuring that the security roles and responsibilities are clearly defined and communicated, that the security personnel are adequately compensated and motivated, and that the security personnel are evaluated and developed regularly. This can help to retain the security talent and expertise, as well as to reduce the costs and risks associated with the security staff turnover12. Information assets are classified appropriately © is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit.
Information asset classification is the process of assigning a security level or category to the information assets based on their value, sensitivity, and criticality to the organization. Aligning the information security program requirements with the employment and staffing processes can help to ensure that the information assets are classified appropriately by establishing the ownership and custody of the information assets, the criteria and methods for the information asset classification, and the roles and responsibilities for the information asset classification. This can help to protect the information assets according to their security level or category, as well as to comply with the regulatory and contractual requirements12. References = 1: CISM Review Manual
15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG)
[2022 update]2

NEW QUESTION: 457
Which of the following is MOST important to include in an information security policy?
A. Management objectives
B. Baselines
C. Maturity levels

D. Best practices
Answer: (SHOW ANSWER)

NEW QUESTION: 458
Which of the following should be done NEXT following senior management's decision to comply with new personal data regulations that are much more stringent than those currently followed to avoid massive fines?
A. Encrypt data in transit and at rest.
B. Complete a return on investment (ROI) analysis.
C. Create and implement a data minimization plan.
D. Conduct a gap analysis.
Answer: (SHOW ANSWER)
A gap analysis is a tool that helps to identify the current state of compliance and the desired state of compliance, as well as the actions needed to achieve the desired state. A gap analysis should be done before implementing any specific controls or solutions, such as encryption, data minimization, or ROI analysis.
References = CISM Review Manual 15th Edition, page 65; Information Security Architecture: Gap Assessment and Prioritization, ISACA Journal, volume 2, 2018.

NEW QUESTION: 459
A serious vulnerability was detected in a business application that can be exploited by external attackers to compromise the system. What is the information security manager's BEST course of action?
A. Ask the business application owner to apply the fix immediately
B. Implement temporary remediation
C. Immediately shut down the application
D. Report the risk to the business application owner
Answer: (SHOW ANSWER)
The best course of action is to implement temporary remediation (B) to reduce exposure while a permanent fix is planned and approved. CISM emphasizes balancing risk reduction with business continuity. Immediate shutdown (C) or unilateral action (A) may disrupt business operations without proper authorization. Reporting the risk (D) is necessary but insufficient on its own. Temporary controls, such as access restrictions or additional monitoring, reduce risk while enabling informed decision-making by the business owner.
References: ISACA CISM Review Manual (Program management-risk response and operational controls); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 460
Penetration testing is MOST appropriate when a:
A. new system is about to go live.
B. new system is being designed.

C. security policy is being developed.
D. security incident has occurred,
Answer: A (LEAVE A REPLY)
= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

NEW QUESTION: 461
Which of the following is the MOST effective way to prevent information security incidents?
A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment
Answer: (SHOW ANSWER)
The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management

(SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

NEW QUESTION: 462
A proposal designed to gain buy-in from senior management for a new security project will be MOST effective if it includes:
A. historical data of reported incidents.
B. industry benchmarking gap analysis.
C. projected return on investment (ROI).
D. analysis of current threat landscape.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 463
Which of the following MUST happen immediately following the identification of a malware incident?
A. Preparation
B. Recovery
C. Containment
D. Eradication
Answer: C (LEAVE A REPLY)
Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident12. Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently12. Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure12. Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware incident12. References = 1: CISM

Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA2

NEW QUESTION: 464
To prepare for a third-party forensics investigation following an incident involving malware, the incident response team should:
A. isolate the infected systems.
B. preserve the evidence.
C. image the infected systems.
D. clean the malware.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the incident response team should preserve the evidence as the first step to prepare for a third-party forensics investigation, as it helps to maintain the integrity and admissibility of the evidence in a court of law. Preserving the evidence may include isolating and imaging the infected systems, but these are not the only actions required. Cleaning the malware may destroy or alter the evidence and should be avoided until the investigation is completed.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.6.2, page 165

NEW QUESTION: 465
The MOST important reason to classify security incidents is to:
A. Improve the efficiency and effectiveness of incident resolution
B. Better manage security event and incident logging
C. Align the incident response plan with corporate policy
D. Enhance the reporting of incident status to the incident lead
Answer: (SHOW ANSWER)
The correct answer is A because incident classification enables the organization to prioritize, escalate, assign, and resolve incidents efficiently and effectively. Classification helps determine severity, business impact, required response time, communication needs, legal or regulatory involvement, evidence handling, and appropriate containment actions. Without classification, all incidents may be treated the same, which can waste resources on low-risk events or delay response to high-impact incidents. Better logging is useful, but it is not the most important reason for classification. Aligning the incident response plan with corporate policy is important during plan development, not the primary purpose of classifying individual incidents. Reporting incident status to the incident lead may be improved through classification, but that is a supporting benefit.
CISM incident management principles emphasize that incidents must be identified, categorized, prioritized, escalated, and resolved based on business impact and risk. Proper classification ensures that resources are directed to the most important incidents and that response actions are appropriate.
Reference: CISM Information Security Incident Management; incident classification, prioritization, escalation, severity, and resolution principles.

NEW QUESTION: 466
Which of the following is the PRIMARY purpose of an acceptable use policy?
A. To provide steps for carrying out security-related procedures
B. To facilitate enforcement of security process workflows
C. To protect the organization from misuse of information assets
D. To provide minimum security baselines for information assets
Answer: (SHOW ANSWER)
The PRIMARY purpose of an acceptable use policy is to protect the organization from misuse of information assets, such as data, hardware, software, and network resources, by defining the rules and expectations for the authorized and appropriate use of these assets by the users. An acceptable use policy helps to prevent or reduce the risks of security breaches, legal liabilities, reputational damage, or loss of productivity that may result from unauthorized, inappropriate, or unethical use of information assets.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 74: "An acceptable use policy is a policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet." The essentials of an acceptable use policy - Infosec Resources: "An Acceptable Use Policy (henceforward mentioned as "AUP") is agreement between two or more parties to a computer network community, expressing in writing their intent to adhere to certain standards of behaviour with respect to the proper usage of specific hardware & software services." Acceptable use policy template - Workable: "This Acceptable Use Policy sets the minimum requirements for the use of our company's IT resources, including computers, networks, devices, software, and internet. It aims to protect our company and our employees from harm and liability, and to ensure that our IT resources are used appropriately, productively, and securely."

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 467
Which of the following is the MOST important consideration when developing key performance indicators (KPIs) for the information security program?
A. Alignment with financial reporting
B. Alignment with business initiatives

C. Alignment with industry frameworks
D. Alignment with risk appetite
Answer: (SHOW ANSWER)
Explore
The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain - Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

NEW QUESTION: 468
Which of the following is the GREATEST threat posed by quantum computing technology for information security?
A. Quantum computers can break several current encryption schemes protecting the confidentiality of data
B. Quantum computers can allow for secure communication that benefits only the few who can afford it
C. Quantum computers can compromise availability through extremely rapid processing of large data sets
D. Quantum computers can simulate complex physical systems beyond traditional computing capabilities
Answer: (SHOW ANSWER)
The greatest threat posed by quantum computing is its potential to break widely used cryptographic algorithms (A), particularly public-key encryption schemes that rely on mathematical problems vulnerable to quantum algorithms. This directly threatens data confidentiality and long-term data protection. The other options describe secondary or non-security impacts. CISM recognizes cryptographic resilience as a core component of risk management and emphasizes the need for organizations to monitor emerging technologies that

could invalidate existing controls. Quantum computing's impact on encryption represents a systemic risk to trust, privacy, and secure communications.
References: ISACA CISM Review Manual (Risk management-emerging technologies and cryptographic risk); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 469
Which of the following is MOST important for the improvement of a business continuity plan (BCP)?
A. Implementing management reviews
B. Documenting critical business processes
C. Implementing an IT resilience solution
D. Incorporating lessons learned
Answer: (SHOW ANSWER)

NEW QUESTION: 470
An organization is evaluating mobile device management software for use in a bring your own device environment. The MOST important feature of the mobile device management software would be the ability to:
Freecram.net
A. Block network access
B. Track device location
C. Enable remote wipe
D. Retain text messages
Answer: (SHOW ANSWER)
The correct answer is C because remote wipe is one of the most important mobile device management features in a bring your own device environment. BYOD devices may be lost, stolen, compromised, or used after an employee leaves the organization. Remote wipe allows the organization to remove corporate data from a device to reduce the risk of unauthorized disclosure. This is especially important because the device is personally owned and may not be fully controlled by the organization. Blocking network access can help prevent future connectivity, but it does not remove sensitive data already stored on the device. Tracking device location may raise privacy concerns and does not directly protect organizational information. Retaining text messages is generally not a primary security requirement and may create privacy or legal concerns. In CISM risk management, mobile controls should protect information while balancing user privacy and business needs. Remote wipe best addresses the risk of corporate data exposure on BYOD devices.
Reference: CISM Information Risk Management; BYOD risk, mobile device management, data protection, remote wipe, and endpoint security principles.

NEW QUESTION: 471
Which of the following elements of a service contract would BEST enable an organization to monitor the information security risk associated with a cloud service provider?

A. Indemnification clause
B. Breach detection and notification
C. Compliance status reporting
D. Physical access to service provider premises
Answer: (SHOW ANSWER)
Compliance status reporting is the best element of a service contract that would enable an organization to monitor the information security risk associated with a cloud service provider, as it provides the organization with regular and timely information on the cloud service provider's compliance with the agreed-upon security requirements, standards, and regulations. Compliance status reporting also helps the organization to identify any gaps or issues that need to be addressed or resolved, and to verify the effectiveness of the cloud service provider's controls. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 472
A daily monitoring report reveals that an IT employee made a change to a firewall rule outside of the change control process. The information security manager's FIRST step in addressing the issue should be to:
A. require that the change be reversed
B. review the change management process
C. perform an analysis of the change
D. report the event to senior management
Answer: (SHOW ANSWER)
Performing an analysis of the change is the first step in addressing the issue of an IT employee making a change to a firewall rule outside of the change control process because it helps to understand the reason, impact, and risk of the change and to decide whether to approve, reject, or reverse it. Requiring that the change be reversed is not the first step because it may cause more disruption or damage without proper analysis and testing. Reviewing the change management process is not the first step because it does not address the specific issue or incident at hand, but rather focuses on improving the process for future changes.
Reporting the event to senior management is not the first step because it does not resolve the issue or incident, but rather escalates it without sufficient information or recommendation.
References: https://www.isaca.org
/resources/isaca-journal/issues/2018/volume-3/change-management-in-the-age-of-digital-transformation
https://www.isaca.org/resources/isaca-journal/issues/

NEW QUESTION: 473
Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?

A. Include security requirements in the contract.
B. Update the risk register.
C. Consult with the business owner.
D. Restrict application network access temporarily.
Answer: (SHOW ANSWER)
Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: "The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications." CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third- party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk." Best Practices to Manage Risks in the Cloud - ISACA: "The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance."

NEW QUESTION: 474
The MOST significant security issue resulting from the growth in the number of mobile devices and an increase in their flexibility is the:
A. Higher exposure to threats
B. Lack of accountability
C. Complexity of support
D. Diversity of operating systems
Answer: (SHOW ANSWER)
The correct answer is A because the growth and flexibility of mobile devices significantly increases the organization's exposure to threats. Mobile devices are portable, often connect through untrusted networks, may store sensitive business data, and can be lost, stolen, compromised, or used outside normal corporate controls. Their flexibility allows users to access organizational resources from many locations, devices, and network environments, which expands the attack surface. Lack of accountability may be a concern in some bring your own device environments, but it can be addressed through policies, mobile device management, logging, and access controls. Complexity of support and diversity of operating systems are

operational challenges, but they are secondary to the broader security issue of increased threat exposure. CISM risk management focuses on identifying how technology changes affect the organization's risk profile. As mobile usage grows, the organization faces more opportunities for malware, unauthorized access, data leakage, insecure applications, and device compromise. Therefore, higher exposure to threats is the most significant issue.
Reference: CISM Information Risk Management; mobile device risk, BYOD, threat exposure, endpoint security, and attack surface management principles.

NEW QUESTION: 475
Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?
A. Availability of resources
B. Root cause analysis results
C. Adverse effects on the business
D. Legal and regulatory requirements
Answer: (SHOW ANSWER)
The severity hierarchy for information security incident classification should be based on the potential or actual impact of the incident on the business objectives, operations, reputation, and stakeholders. The adverse effects on the business can be measured by criteria such as financial loss, operational disruption, legal liability, regulatory compliance, customer satisfaction, and public confidence. The other options are not the primary basis for a severity hierarchy, although they may be considered as secondary factors or consequences of an incident

NEW QUESTION: 476
Which of the following is MOST likely to reduce the effectiveness of a SIEM system?
A. Complex user interface
B. Misconfiguration of alert thresholds
C. Weakly encrypted log files
D. Lack of multi-factor authentication (MFA) for system access
Answer: (SHOW ANSWER)
The effectiveness of a SIEM (Security Information and Event Management) system heavily relies on properly configured alert thresholds. Misconfiguration of alert thresholds can result in missed detection of significant incidents (false negatives) or an overwhelming number of false positives, making it difficult to identify real threats. According to the CISM Review Manual, 16th Edition, Domain 4: Information Security Incident Management, the configuration and tuning of monitoring tools like SIEMs are crucial for timely and accurate detection of incidents.
Reference:ISACA CISM Review Manual, 16th Edition, Page 304-305, "Security Event Management Tools and Techniques".

NEW QUESTION: 477
Which of the following is the MOST important detail to capture in an organization's risk register?

A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria
D. Risk ownership
Answer: D (LEAVE A REPLY)
Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

NEW QUESTION: 478
Which of the following is the MOST effective way to detect information security incidents?
A. Periodic analysis of security event log records
B. Threshold settings on key risk indicators (KRIs)
C. Implementation of regular security awareness programs
D. Real-time monitoring of network activity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 479
An information security manager has been notified that two senior executives have the ability to elevate their own privileges in the corporate accounting system, in violation of policy. What is the FIRST step to address this issue?
A. Perform a full review of all system transactions over the past 90 days.
B. Perform a system access review.
C. Notify the CISO of the security policy violation.
D. Immediately suspend the executives' access privileges.
Answer: (SHOW ANSWER)

NEW QUESTION: 480
Who is BEST positioned to take ownership of critical IT security risks identified in an application?
A. Chief information officer (CIO)
B. Chief information security officer (CISO)
C. Business application owner
D. Lead application developer
Answer: (SHOW ANSWER)
The business application owner (C) is best positioned to own application-related security risks because they are accountable for the business outcomes, value, and operational impact of the application. CISM consistently assigns risk ownership to business roles, not technical implementers. The CISO (B) advises on security posture, the CIO (A) oversees IT strategy, and

developers (D) implement controls-but none are accountable for accepting or prioritizing business risk. Assigning ownership to the application owner ensures that risk decisions reflect business priorities and align with risk appetite.
References: ISACA CISM Review Manual (Governance-risk ownership and accountability); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 481
An organization that has recently suffered a cyberattack is considering engaging law enforcement. Which of the following is the MOST important course of action for the incident response team?
A. Encrypt digital evidence
B. Solicit input from senior management
C. Engage legal counsel
D. Hire a digital forensic expert for evidence analysis
Answer: C (LEAVE A REPLY)
The most important course of action before engaging law enforcement is to engage legal counsel. In CISM incident management, legal counsel helps ensure that the organization complies with legal obligations, preserves privilege where applicable, understands reporting requirements, and avoids actions that could create additional liability. Cyberattacks may involve privacy laws, contractual notification requirements, regulatory obligations, evidence handling requirements, and possible criminal proceedings. Legal counsel is best positioned to advise whether and how law enforcement should be involved. Encrypting evidence is not the primary concern and could complicate evidence handling if not done properly. Senior management input is important, but legal guidance is essential when external authorities may be involved. Hiring forensic experts may also be necessary, but legal counsel should guide the scope, engagement, evidence handling, and reporting considerations. CISM emphasizes coordinated incident response involving legal, communications, management, and technical teams. Therefore, engaging legal counsel is the most important action when law enforcement involvement is being considered.
References:
ISACA CISM Review Manual, Information Security Incident Management - legal considerations and external reporting ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here:

https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 482
Which of the following would BEST help to ensure appropriate security controls are built into software?
A. Integrating security throughout the development process
B. Performing security testing prior to deployment
C. Providing standards for implementation during development activities
D. Providing security training to the software development team
Answer: (SHOW ANSWER)
The best way to ensure appropriate security controls are built into software is to integrate security throughout the development process. This means that security should be considered from the initial stages of planning, design, coding, testing, deployment, and maintenance of the software. Integrating security throughout the development process helps to identify and mitigate security risks early, reduce the cost and complexity of fixing vulnerabilities later, improve the quality and reliability of the software, and enhance the trust and confidence of the users and customers. Integrating security throughout the development process also aligns with the best practices and standards of information security governance, such as the CISM framework123.
References =
CISM Review Manual 15th Edition, page 1631
CISM domain 3: Information security program development and management [2022 update]2
CISSP domain 8 overview: Software development security4

NEW QUESTION: 483
Which of the following BEST supports information security management in the event of organizational changes in security personnel?
A. Formalizing a security strategy and program
B. Developing an awareness program for staff
C. Ensuring current documentation of security processes
D. Establishing processes within the security operations team
Answer: (SHOW ANSWER)
Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational

changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION: 484
Of the following, who is BEST positioned to be accountable for risk acceptance decisions based on risk appetite?
A. Information security manager
B. Chief risk officer (CRO)
C. Information security steering committee
D. Risk owner
Answer: D (LEAVE A REPLY)
The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.
References = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

NEW QUESTION: 485
Which of the following is the PRIMARY objective of testing security controls within a critical infrastructure?
A. Identifying and addressing security team performance issues
B. Ensuring the continued resilience and security of IT services
C. Decreasing the percentage of security deployments that cause failures in production
D. Reducing the number of control assessments to optimize resources
Answer: (SHOW ANSWER)
The correct answer is B because the primary objective of testing security controls in critical infrastructure is to ensure that IT services remain secure, resilient, and available. Critical infrastructure supports essential business, public, or operational services, so control failures may have severe consequences. Testing verifies whether controls are designed and operating effectively, whether they reduce risk as intended, and whether they support continuity of critical services. Identifying security team performance issues may be a secondary outcome of testing, but it is not the primary objective. Reducing failed deployments is useful for operational quality, but security control testing focuses on assurance and resilience rather than deployment statistics. Reducing the number of assessments may save resources, but fewer assessments do not necessarily improve security. In CISM program management, controls must be monitored and tested to ensure they continue to meet control objectives and support business requirements. For critical infrastructure, resilience and security of services are the central goals.

Reference: CISM Information Security Program Development and Management; control testing, critical infrastructure protection, resilience, and service security principles.

NEW QUESTION: 486
An international organization with remote branches is implementing a corporate security policy for managing personally identifiable information (PII). Which of the following should be the information security manager's MAIN concern?
A. Local regulations
B. Data backup strategy
C. Consistency in awareness programs
D. Organizational reporting structure
Answer: (SHOW ANSWER)
Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

NEW QUESTION: 487
Which of the following is MOST important to the successful implementation of an information security program?
A. Adequate security resources are allocated to the program.
B. Key performance indicators (KPIs) are defined.
C. A balanced scorecard is approved by the steering committee.
D. The program is developed using global security standards.
Answer: (SHOW ANSWER)
The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives, comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.
References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 488

An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:
* A bad actor broke into a business-critical FTP server by brute forcing an administrative password
* The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
* The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
* After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail Which of the following could have been prevented by conducting regular incident response testing?
A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data
Answer: (SHOW ANSWER)
Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. References: https://www.isaca.org/resources/isaca-journal/issues/2017
/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 489
If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:
A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.
Answer: (SHOW ANSWER)
Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and

admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court. The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12. Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server- backup utilities © is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody.
Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks involved in the incident, but it may also introduce changes or errors that could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12.
Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files, or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4:
Information Security Incident Management (ISIM) [2022 update]2

NEW QUESTION: 490

Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?

Freeclam.net

A. Information security incidents
B. Availability of potential resources
C. Information security strategy
D. Current resourcing levels
Answer: (SHOW ANSWER)

NEW QUESTION: 491

Which type of recovery site is MOST reliable and can support stringent recovery requirements?
A. Cold site
B. Warm site
C. Hot site
D. Mobile site
Answer: (SHOW ANSWER)
A hot site is the most reliable type of recovery site and can support stringent recovery requirements because it is a fully operational facility that mirrors the primary production center. A hot site has all the hardware, software, data, network, and personnel ready to resume the critical business functions within minutes of a disruptive event. A hot site also has backup power, security, and communication systems to ensure the continuity of operations.
References: The CISM Review Manual 2023 defines a hot site as "a fully operational facility that mirrors the primary production center" and states that "a hot site can support stringent recovery requirements and provide the shortest recovery time" (p. 190). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A hot site is the correct answer because it is the most reliable type of recovery site and can support stringent recovery requirements, as it is a fully operational facility that mirrors the primary production center and can resume the critical business functions within minutes of a disruptive event" (p. 96). Additionally, the web search result 1 states that "the recovery site can be hot, warm, cold or mobile. Hot sites are facilities that mirror the primary production center" and that "hot sites are the most reliable and can support stringent recovery requirements" (p. 1).

NEW QUESTION: 492
Which of the following would BEST guide the development and maintenance of an information security program?
A. A business impact assessment
B. A comprehensive risk register
C. An established risk assessment process
D. The organization's risk appetite
Answer: (SHOW ANSWER)
According to the CISM Manual, the organization's risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives1. The organization's risk appetite should guide the development and maintenance of an information security program, as it determines the level of security controls, resources, and activities that are needed to protect the organization's assets and operations1.
The CISM Manual states that "the information security program should be aligned with the organization's risk appetite, which reflects its tolerance for risk and its strategic objectives" (IR 8288A)1. The information security program should also consider other factors that influence the organization's risk appetite, such as its mission, vision, values, culture, stakeholders, regulations, standards, guidelines, and best practices1.

The CISM Manual also provides guidance on how to develop and maintain an information security program based on the organization's risk appetite. It recommends using a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that affect the organization's information assets1. It also suggests using a framework or model that supports the development of an information security program based on the organization's risk appetite (e.g., ISO/IEC 27001)1.
References: 1: IR 8288A - Information Security Program Development | CSRC NIST

NEW QUESTION: 493
An organization has suffered from a large-scale security event impacting a critical system. Following the decision to restore the system at an alternate location, which plan should be invoked?
A. Disaster recovery plan (DRP)
B. Communications plan
C. Business continuity plan (BCP)
D. Incident response plan
Answer: (SHOW ANSWER)

Valid CISM Dumps shared by ExamDiscuss.com for Helping Passing CISM Exam! ExamDiscuss.com now offer the **newest CISM exam dumps**, the ExamDiscuss.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CISM dumps with Test Engine here: https://www.examdiscuss.com/ISACA/exam/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)