

ISACA.CISM.v2026-10-07.q489

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	489
Version:	v2026-10-07
# of views:	103
# of Questions views:	4890
https://www.freecram.net/torrent/ISACA.CISM.v2026-10-07.q489.html	

NEW QUESTION: 1

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 incident 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 coordination

- *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 components of an effective incident response capability². The other options are not the primary 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 incident. 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 security incident? - TechTarget : 10 types of security incidents and how to handle them
- TechTarget : 45 CFR § 164.304 - Definitions - Electronic Code of Federal Regulations

NEW QUESTION: 2

Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

- A.** Communicate disciplinary processes for policy violations.
- B.** Require staff to participate in information security awareness training.
- C.** Require staff to sign confidentiality agreements.
- D.** Include information security responsibilities in job descriptions.

Answer: ([SHOW ANSWER](#))

The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3:

Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION: 3

In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:

- A.** change activities are documented.
- B.** the rationale for acceptance is periodically reviewed.
- C.** the acceptance is aligned with business strategy.
- D.** compliance with the risk acceptance framework.

Answer: ([SHOW ANSWER](#))

= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with

the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.

References =

CISM Review Manual 15th Edition, page 1131

CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482 CISM Domain 2: Information Risk Management (IRM) [2022 update]³

NEW QUESTION: 4

Which of the following is the PRIMARY advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program?

- A.** It offers the organization flexible deployment options using cloud infrastructure.
- B.** It allows the organization to prioritize its core operations.
- C.** It is more secure than traditional data backup architecture.
- D.** It allows the use of a professional response team at a lower cost.

Answer: ([SHOW ANSWER](#))

The primary advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program is B. It allows the organization to prioritize its core operations. This is because DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster¹. DRaaS can help the organization to prioritize its core operations by:

Reducing the need for provisioning and maintaining its own off-site disaster recovery environment, which can be costly, complex, and resource-intensive¹² Enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers, which can minimize the downtime, data loss, and business disruption¹² Providing the organization with flexible and scalable deployment options, such as on-demand, pay-per-use, or subscription-based models, that can meet its changing business needs and budget¹² Leveraging the expertise, experience, and best practices of the service provider, who can handle the disaster recovery planning, testing, and execution, and ensure compliance with the relevant standards and regulations¹² DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. DRaaS can help the organization to prioritize its core operations by reducing the need for provisioning and maintaining its own off-site disaster recovery environment, enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment, providing the organization with flexible and scalable deployment options, and

leveraging the expertise, experience, and best practices of the service provider. (From CISM Manual or related resources)

NEW QUESTION: 5

When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?

- A.** Business process owner
- B.** Business continuity coordinator
- C.** Senior management
- D.** Information security manager

Answer: ([SHOW ANSWER](#))

The business process owner 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 business process owner has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the business process owner is the best person to calculate the recovery time and cost estimates when performing a business impact analysis (BIA), which is a process of identifying and quantifying the potential losses, damages, or consequences that could result from 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 recovery time and cost estimates are the measures that indicate the time and money that are needed to resume and restore the normal business operations and functions after the disruption or incident. The recovery time and cost estimates can help to prioritize and protect the critical activities and resources, to allocate the appropriate budget and resources, to implement the necessary controls and measures, and to evaluate the effectiveness and efficiency of the business continuity and disaster recovery plans.

The business continuity coordinator, the senior management, and the information security manager are all important roles in the BIA process, but they are not the best ones to calculate the recovery time and cost estimates. The business continuity coordinator is the person who is responsible for coordinating and facilitating the BIA process, as well as the development, implementation, and maintenance of the business continuity and disaster recovery plans. The business continuity coordinator can help to define and communicate the scope, objectives, and methodology of the BIA, to collect and analyze the data and information from the business process owners and other stakeholders, to report and present the BIA results and recommendations, and to provide feedback and suggestions for improvement and optimization of the BIA and the plans. The senior management is the group of people who have the ultimate authority and accountability for the organization's strategy, direction, and performance. The senior management can help to approve and support the BIA process and the plans, to provide the strategic guidance and vision for the business continuity and disaster recovery, to allocate the necessary budget and resources, to oversee and monitor the BIA and the plans, and to make the final decisions and approvals. The information security manager is the person who is responsible

for ensuring the security of the information assets and systems that support the business processes and functions. The information security manager can help to identify and assess the information security risks and issues that could affect the BIA and the plans, to implement and manage the security controls and measures that are needed to protect and recover the information assets and systems, to coordinate and collaborate with the business process owners and other stakeholders on the security aspects of the BIA and the plans, and to provide the security expertise and advice. References = CISM Review Manual 15th Edition, pages 228-2291; CISM Practice Quiz, question 1722

NEW QUESTION: 6

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

- 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: 7

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: 8

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: 9

Which of the following is MOST helpful for aligning security operations with the IT governance framework?

- A. Security risk assessment
- B. Security operations program
- C. Information security policy
- D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

An information security policy is the MOST helpful for aligning security operations with the IT governance framework because it defines the security objectives, principles, standards, and guidelines that guide the security operations activities and processes. An information security policy also establishes the roles and responsibilities, authorities and accountabilities, and reporting and communication mechanisms for security operations. An information security policy should be aligned with the IT governance framework, which provides the direction, structure, and oversight for the effective management and delivery of IT services and resources. An information security policy should also be consistent with the enterprise governance framework, which sets the vision, mission, values, and goals of the organization¹². A security risk assessment (A) is helpful for identifying and evaluating the security risks that may affect the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A security risk assessment should be based on the information security policy, which defines the risk appetite, tolerance, and criteria for the organization¹². A security operations program (B) is helpful for implementing and executing the security operations activities and processes that support the IT governance framework, but it is not the MOST helpful for aligning them. A security operations program should be derived from the information security policy, which provides the strategic direction and guidance for the security operations¹². A business impact analysis (BIA) (D) is helpful for determining the criticality and priority of the business processes and functions that depend on the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A BIA should be conducted in accordance with the information security policy, which specifies the business continuity and disaster recovery requirements and objectives for the organization¹². 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: 10

To align with the principles of Zero Trust, which of the following is the MOST important course of action when engaging with external parties?

- A. Requiring external parties to use a specific type of encryption for data at rest and in transit
- B. Insisting on regular comprehensive audits of external parties' access management practices
- C. Ensuring contracts with external parties mandate continuous verification and least privilege access
- D. Mandating that external parties provide annual security training to their employees

Answer: ([SHOW ANSWER](#))

The most important action aligned with Zero Trust principles is ensuring contracts with external parties mandate continuous verification and least privilege access. Zero Trust is based on the principle of "never trust, always verify," requiring ongoing validation of identity, device posture, access context, and authorization. It also requires limiting access to the minimum necessary for the task. Encryption, audits, and annual training are valuable supporting controls, but they do not capture the core operating model of Zero Trust as directly as continuous verification and least privilege. When engaging external parties, contractual requirements are essential because they create enforceable obligations for how access to organizational systems and data must be managed. CISM governance principles emphasize that third-party access should be controlled through documented requirements, accountability, monitoring, and risk-based oversight. Therefore, the best answer is mandating continuous verification and least privilege access in contracts, because this embeds Zero Trust expectations into third-party governance and access management.

References:

ISACA CISM Review Manual , Information Security Governance - third-party access control and security requirements ISACA CISM Exam Content Outline , Domain 2: Information Security Governance

NEW QUESTION: 11

Which of the following BEST supports effective communication during information security incidents?

- A. Frequent incident response training sessions
- B. Centralized control monitoring capabilities
- C. Responsibilities defined within role descriptions
- D. Predetermined service level agreements (SLAs)

Answer: ([SHOW ANSWER](#))

The best way to support effective communication during information security incidents is to have predetermined service level agreements (SLAs) because they define the expectations and responsibilities of the parties involved in the incident response process, and specify the communication channels, methods, and frequency for reporting and updating on the incident status and resolution. Frequent incident response training sessions are not very effective because they do not address the communication needs or challenges during an actual incident. Centralized control monitoring capabilities are not very effective because they do not address the

communication needs or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or challenges during an actual 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: 12

Which of the following is MOST important when developing an AI security awareness program?

- A. Creating an interactive training environment
- B. Aligning the training to user roles
- C. Defining the level of user interaction with AI
- D. Assessing the maturity of the organization

Answer: (SHOW ANSWER)

The correct answer is B because awareness training is most effective when it is aligned with user roles, responsibilities, and exposure to risk. An AI security awareness program should address how different users interact with AI tools, what data they may enter, what decisions they may make, and what risks apply to their specific functions. For example, developers, executives, analysts, HR staff, legal teams, and general users may face different AI-related risks. Interactive training can improve engagement, but it is not more important than relevance to the user's role. Defining the level of interaction with AI is useful input for tailoring the program, but the broader objective is role-based training. Assessing organizational maturity may help planning, but it does not ensure users receive relevant guidance. CISM program management emphasizes awareness and training appropriate to roles and responsibilities. Therefore, aligning training to user roles is the most important consideration.

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

NEW QUESTION: 13

Which of the following is the BEST defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns?

- A. Compartmentalization
- B. Overlapping redundancy
- C. Continuous monitoring
- D. Multi-factor authentication

Answer: (SHOW ANSWER)

Compartmentalization is the best defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns because it is a strategy that divides the network or system into smaller segments or compartments, each with its own security policies, controls, and access rules.

Compartmentalization helps to isolate and protect the most sensitive or critical data and functions from unauthorized or malicious access, as well as to limit the damage or impact of a breach or compromise.

Compartmentalization also helps to enforce the principle of least privilege, which grants users or processes only the minimum access rights they need to perform their tasks. Therefore, compartmentalization is the correct answer.

References:

* <https://www.csoonline.com/article/3667476/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html>

* <https://www.fortinet.com/resources/cyberglossary/defense-in-depth>

* <https://sciencepublishinggroup.com/journal/paperinfo?journalid=542&doi=10.11648/j.ajai.20190302.11>

NEW QUESTION: 14

Which of the following is the BEST way to align security and business strategies?

- A. Establish key performance indicators for the business
- B. Integrate information security governance into corporate governance
- C. Ensure the information security program conforms to industry standards
- D. Include security risk as part of ongoing metrics reporting

Answer: (SHOW ANSWER)

The correct answer is B because integrating information security governance into corporate governance ensures that security decisions are made as part of overall business direction, risk management, investment, and accountability. Security strategy should not operate separately from enterprise strategy. When information security governance is embedded in corporate governance, security objectives are aligned with business objectives, risk appetite, regulatory obligations, and stakeholder expectations. Establishing business KPIs may help measure business performance, but it does not directly align security strategy. Conformance to industry standards can improve maturity and consistency, but standards may not fully reflect the organization's unique business priorities. Reporting security risk in metrics is useful, but reporting alone does not create strategic alignment. CISM emphasizes that information security must support enterprise objectives and be governed through appropriate structures, roles, and oversight. Therefore, integrating information security governance into corporate governance is the best way to align security and business strategies.

Reference: CISM Information Security Governance; corporate governance integration, strategic alignment, enterprise risk, and accountability principles.

NEW QUESTION: 15

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: 16

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.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

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: 18

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: 19

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: 20

A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems. The vendor has released an emergency patch. Which of the following should be the information security managers PRIMARY concern?

- A. Availability of resources to implement controls
- B. Documentation of patching procedures
- C. Ability to test the patch prior to deployment
- D. Adequacy of the incident response plan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 21

An information security manager developing an incident response plan MUST ensure it includes:

- A. an inventory of critical data.
- B. criteria for escalation.
- C. a business impact analysis (BIA).
- D. critical infrastructure diagrams.

Answer: B ([LEAVE A REPLY](#))

An incident response plan is a set of procedures and guidelines that define the roles and responsibilities of the incident response team, the steps to follow in the event of an incident, and the communication and escalation protocols to ensure timely and effective resolution of incidents. One of the essential components of an incident response plan is the criteria for escalation, which specify the conditions and thresholds that trigger the escalation of an incident to a higher level of authority or a different function within the organization. The criteria for escalation may depend on factors such as the severity, impact, duration, scope, and complexity of the incident, as well as the availability and capability of the incident response team. The criteria for escalation help to ensure that incidents are handled by the appropriate personnel, that management is kept informed and involved, and that the necessary resources and support are provided to resolve the incident. References = <https://blog.exigence.io/a-practical-approach-to-incident-management-escalation>

<https://www.uc.edu/content/dam/uc/infosec/docs/Guidelines>

[/Information_Security_Incident_Response_Escalation_Guideline.pdf](#)

NEW QUESTION: 22

Which of the following should be implemented to BEST reduce the likelihood of a security breach?

- A. A layered security program
- B. An incident response program
- C. A configuration management program
- D. A data forensics program

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

Which of the following activities is MOST appropriate to conduct during the eradication phase of a cyber incident response?

- A. Mitigate exploited vulnerabilities to stop future incidents.
- B. Estimate the amount of damage caused by the incident.
- C. Restore affected systems for normal operations.
- D. Isolate affected systems to prevent further damage

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 24

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 25

Which of the following has The GREATEST positive impact on The ability to execute a disaster recovery plan (DRP)?

- A. Storing the plan at an offsite location
- B. Communicating the plan to all stakeholders
- C. Updating the plan periodically
- D. Conducting a walk-through of the plan

Answer: ([SHOW ANSWER](#))

A walk-through of the disaster recovery plan (DRP) is a method of testing the plan by simulating a disaster scenario and having the participants review their roles and responsibilities, as well as the procedures and resources required to execute the plan. A walk-through has the greatest positive impact on the ability to execute the DRP, as it helps to identify and resolve any gaps, errors, or inconsistencies in the plan, as well as to enhance the awareness and readiness of the stakeholders involved in the recovery process. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.3.2.21

NEW QUESTION: 26

Which of the following is the MOST effective way to convey information security responsibilities across an organization?

- A. Implementing security awareness programs
- B. Documenting information security responsibilities within job descriptions
- C. Developing a skills matrix
- D. Defining information security responsibilities in the security policy

Answer: ([SHOW ANSWER](#))

Documenting information security responsibilities within job descriptions is the most effective way to convey information security responsibilities across an organization because it clearly defines the roles, expectations, and accountabilities of each employee regarding information security. It also helps to align the information security objectives with the business goals and performance indicators, and to ensure compliance with the security policies and standards.

References = CISM Review Manual 15th Edition, What is CISM? - Digital Guardian

NEW QUESTION: 27

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: 28

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.

NEW QUESTION: 29

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: 30

The contribution of recovery point objective (RPO) to disaster recovery is to:

- A. minimize outage periods.
- B. eliminate single points of failure.
- C. define backup strategy
- D. reduce mean time between failures (MTBF).

Answer: (SHOW ANSWER)

The contribution of recovery point objective (RPO) to disaster recovery is to define backup strategy because it determines the maximum amount of data loss that is acceptable to an organization after a disruption, and guides the frequency and type of backups needed to restore the data to a usable format¹. Minimize outage periods is not a contribution of RPO, but rather a contribution of recovery time objective (RTO), which defines the maximum amount of time that is acceptable to restore normal operations after a disruption². Eliminate single points of failure is not a contribution of RPO, but rather a goal of high availability (HA), which ensures that systems or services are continuously operational and resilient³. Reduce mean time between failures (MTBF) is not a contribution of RPO, but rather a measure of reliability, which indicates the average time that a system or component operates without failure⁴. References: 1 <https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs> 2 <https://www.druva.com>

/glossary/what-is-a-recovery-time-objective-definition-and-related-faqs 3

<https://www.fortinet.com/resources>

/cyberglossary/high-availability 4 <https://www.fortinet.com/resources/cyberglossary/mean-time-between-failures>

NEW QUESTION: 31

Which of the following is MOST important to consider when choosing a shared alternate location for computing facilities?

- A. The organization's risk tolerance
- B. The organization's mission
- C. Resource availability
- D. Incident response team training

Answer: ([SHOW ANSWER](#))

The organization's risk tolerance is the most important factor to consider when choosing a shared alternate location for computing facilities, as it determines the acceptable level of risk exposure and the required recovery time objective (RTO) for the organization. A shared alternate location is a facility that is used by multiple organizations for disaster recovery purposes, and it may have limited resources, availability, and security. Therefore, the organization must assess its risk tolerance and ensure that the shared alternate location can meet its recovery requirements and protect its information assets.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291; CISM Online Review Course, Module 4, Lesson 3, Topic 22; BCMpedia, Alternate Site3

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 32

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: 33

Which of the following is the BEST approach when creating a security policy for a global organization subject to varying laws and regulations?

- A.** Incorporate policy statements derived from third-party standards and benchmarks.
- B.** Adhere to a unique corporate privacy and security standard
- C.** Establish baseline standards for all locations and add supplemental standards as required
- D.** Require that all locations comply with a generally accepted set of industry

Answer: ([SHOW ANSWER](#))

= Creating a security policy for a global organization subject to varying laws and regulations is a challenging task, as it requires balancing the need for consistency, compliance, and flexibility. The best approach is to establish baseline standards for all locations that reflect the organization's overall security objectives, principles, and requirements. These standards should be aligned with the organization's mission, vision, values, and strategy, as well as with the applicable laws and regulations of each location. The baseline standards should also be reviewed and updated periodically to ensure their relevance and effectiveness. Additionally, supplemental standards can be added as required to address specific issues or risks that may arise in different locations or situations. Supplemental standards should be based on the best practices and lessons learned from the baseline standards, as well as on the feedback and input from the stakeholders of each location. References = CISM Review Manual, 16th Edition, page 1001

NEW QUESTION: 34

An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

- A.** Lack of availability
- B.** Lack of accountability
- C.** Improper authorization
- D.** Inadequate authentication

Answer: ([SHOW ANSWER](#))

The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other

options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. References:

<https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam>

<https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices>

<https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam>

NEW QUESTION: 35

As part of incident response activities, the BEST time to begin the recovery process is after:

- A. The eradication phase has been completed
- B. The incident response team has been established
- C. The root cause has been determined
- D. The incident manager has declared the incident

Answer: ([SHOW ANSWER](#))

Recovery should not begin until the eradication phase is complete, meaning all malicious activity, malware, or unauthorized access has been removed. Starting recovery too early may reintroduce threats or result in re-infection.

"Recovery begins after eradication is complete, ensuring a clean environment for restoring services."

- CISM Review Manual 15th Edition, Chapter 4: Incident Response Lifecycle, Section: Recovery Phase*

NEW QUESTION: 36

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: ([SHOW ANSWER](#))

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: 37

A business impact analysis (BIA) BEST enables an organization to establish:

- A. Total cost of ownership (TCO).

- B. Restoration priorities.
- C. Annualized loss expectancy (ALE).
- D. Recovery methods.

Answer: ([SHOW ANSWER](#))

A business impact analysis (BIA) best enables an organization to establish restoration priorities (B). In CISM, the primary purpose of a BIA is to identify critical business processes, assess the impact of disruptions over time, and determine which functions must be restored first to minimize business impact. Restoration priorities are derived from factors such as maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs), all of which are key BIA outputs.

Total cost of ownership (A) is a financial analysis concept unrelated to continuity planning. Annualized loss expectancy (C) is an output of quantitative risk analysis, not a BIA. Recovery methods (D) are defined after restoration priorities are established and are part of business continuity and disaster recovery planning. CISM emphasizes that the BIA provides the business-driven foundation upon which recovery strategies and methods are later selected.

By clearly defining restoration priorities, the BIA ensures that continuity planning aligns with business objectives, risk appetite, and operational resilience requirements.

References:

ISACA CISM Review Manual, Information Security Program Development and Management - Business Impact Analysis (BIA) purpose and outcomes ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 38

An employee who is a remote user has copied financial data from the corporate server to a laptop using virtual private network (VPN) connectivity. Which of the following is the MOST important factor to determine if it should be classified as a data leakage incident?

- A. Review of the audit logs
- B. Ownership of the data
- C. Valid use case
- D. Employee's job role

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

The PRIMARY benefit of integrating information security activities into change management processes is to:

- A. ensure required controls are included in changes.
- B. provide greater accountability for security-related changes in the business.
- C. protect the business from collusion and compliance threats.
- D. protect the organization from unauthorized changes.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

An organization's disaster recovery plan (DRP) is documented and kept at a disaster recovery site. Which of the following is the BEST way to ensure the plan can be carried out in an emergency?

- A. Store disaster recovery documentation in a public cloud.
- B. Maintain an outsourced contact center in another country.
- C. Require disaster recovery documentation be stored with all key decision makers.
- D. Provide annual disaster recovery training to appropriate staff.

Answer: (SHOW ANSWER)

= The best way to ensure that the disaster recovery plan (DRP) can be carried out in an emergency is to provide annual disaster recovery training to the appropriate staff, such as the disaster recovery team, the business process owners, and the IT staff. Disaster recovery training is a process of educating and preparing the staff for their roles, responsibilities, and actions in the event of a disaster that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. Disaster recovery training can help to ensure that the staff are aware, capable, and confident to execute the DRP, as well as to minimize the impact and damage to the business continuity, reputation, and value. Disaster recovery training can also help to evaluate the adequacy, accuracy, and applicability of the DRP, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the disaster recovery process. Disaster recovery training can also help to document and report the training details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the DRP and the training process.

Storing disaster recovery documentation in a public cloud, maintaining an outsourced contact center in another country, and requiring disaster recovery documentation be stored with all key decision makers are all possible ways to ensure the availability and accessibility of the DRP in an emergency, but they are not the best ones. Storing disaster recovery documentation in a public cloud is a process of using a third-party service provider to store and manage the DRP documents online, which can offer benefits such as scalability, flexibility, and cost-efficiency, but also risks such as data breach, data loss, or service disruption. Maintaining an outsourced contact center in another country is a process of using a third-party service provider to handle the communication and coordination of the disaster recovery process with the internal and external stakeholders, such as the customers, partners, or regulators, which can offer benefits such as redundancy, reliability, and expertise, but also risks such as cultural, legal, or contractual issues. Requiring disaster recovery documentation be stored with all key decision makers is a process of ensuring that the senior management and the business process owners have a copy of the DRP documents, which can offer benefits such as accountability, authority, and visibility, but also risks such as inconsistency, duplication, or unauthorized access. References = CISM Review Manual 15th Edition, pages 233-2341; CISM Practice Quiz, question 1602

NEW QUESTION: 41

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: 42

Which of the following is the MOST important characteristic of an effective information security metric?

- A. The metric is frequently reported to senior management.
- B. The metric directly maps to an industry risk management framework.
- C. The metric compares the organization's inherent risk against its risk appetite.
- D. The metric expresses residual risk relative to risk tolerance.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

The categorization of incidents is MOST important for evaluating which of the following?

- A. Appropriate communication channels
- B. Allocation of needed resources
- C. Risk severity and incident priority
- D. Response and containment requirements

Answer: C ([LEAVE A REPLY](#))

The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation.

The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence the allocation of resources, the response and

containment requirements, and the communication channels, but they are not the primary purpose of categorization.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

NEW QUESTION: 44

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: 45

A backdoor has been identified that enabled a cyberattack on an organization's systems.

Integrating which of the following into the software development life cycle would BEST enable the organization to mitigate similar attacks in the future?

- A. Enhanced user acceptance testing (UAT)
- B. Separation of duties
- C. Customized developer training
- D. Vulnerability testing

Answer: ([SHOW ANSWER](#))

Integrating vulnerability testing (D) into the SDLC is the most effective way to identify backdoors and security weaknesses before deployment. CISM emphasizes secure development practices, including testing and validation, as essential controls. UAT (A) focuses on functionality, separation of duties (B) addresses governance, and training (C) is supportive but insufficient on its own. Vulnerability testing provides direct detection of exploitable flaws.

References: ISACA CISM Review Manual (Program management-secure SDLC practices); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 46

An employee clicked on a link in a phishing email, triggering a ransomware attack Which of the following should be the information security?

- A. Wipe the affected system.
- B. Notify internal legal counsel.

- C. Notify senior management.
- D. Isolate the impacted endpoints.

Answer: ([SHOW ANSWER](#))

Isolating the impacted endpoints is the best course of action for the information security manager after an employee clicked on a link in a phishing email, triggering a ransomware attack because it prevents the ransomware from spreading to other systems or devices on the network, and minimizes the damage or disruption caused by the attack. Wiping the affected system is not a good course of action because it may destroy any evidence or data that could be used for investigation or recovery. Notifying internal legal counsel is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Notifying senior management is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. 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>

[/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned](https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned)

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

NEW QUESTION: 47

The PRIMARY reason to properly classify information assets is to determine:

- A. the business impact if assets are compromised.
- B. the appropriate protection based on sensitivity.
- C. appropriate encryption strength using a risk-based approach.
- D. user access levels based on the need to know.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 48

Information security policies should PRIMARILY reflect alignment with:

- A. senior management intent.
- B. an information security framework.
- C. data security standards.
- D. industry best practices.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

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 strategy
- B. Information security objectives
- C. Information security threat profile
- D. Information security policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

Which of the following BEST ensures timely and reliable access to services?

- A. Nonrepudiation
- B. Authenticity
- C. Availability
- D. Recovery time objective (RTO)

Answer: ([SHOW ANSWER](#))

= According to the CISM Review Manual, availability is the degree to which information and systems are accessible to authorized users in a timely and reliable manner¹. Availability ensures that services are delivered to the users as expected and agreed upon. Nonrepudiation is the ability to prove the occurrence of a claimed event or action and its originating entities¹. It ensures that the parties involved in a transaction cannot deny their involvement. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication¹. It ensures that the identity of a subject or resource is valid. Recovery time objective (RTO) is the maximum acceptable period of time that can elapse before the unavailability of a business function severely impacts the organization¹. It is a metric used to measure the recovery capability of a system or service, not a factor that ensures timely and reliable access to services. References = CISM Review Manual, 16th Edition, Chapter 2, Information Risk Management, pages 66-67.

NEW QUESTION: 51

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: 52

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: 53

Which risk is introduced when using only sanitized data for the testing of applications?

- A. Data loss may occur during the testing phase.
- B. Data disclosure may occur during the migration event
- C. Unexpected outcomes may arise in production
- D. Breaches of compliance obligations will occur.

Answer: ([SHOW ANSWER](#))

Unexpected outcomes may arise in production when using only sanitized data for the testing of applications.

Sanitized data is data that has been purposely and permanently deleted or modified to prevent unauthorized access or misuse. Sanitized data may not reflect the real characteristics, patterns, or behaviors of the original data, and thus may not be suitable for testing applications that rely on data quality and accuracy. According to NIST, data sanitization methods can affect the usability of data for testing purposes¹. The other options are not risks introduced by using sanitized data for testing applications, but rather risks that can be mitigated by using sanitized data. Data loss, data

disclosure, and breaches of compliance obligations are possible consequences of using unsanitized data that contains sensitive or confidential information. References: 2: What is Data Sanitization? | Data Erasure Methods | Imperva 3: Data sanitization techniques: Standards, practices, legislation 1: Data sanitization - Wikipedia

NEW QUESTION: 54

Which of the following is MOST important to consider when determining backup frequency?

- A. Allowable interruption window
- B. Recovery time objective (RTO)
- C. Recovery point objective (RPO)
- D. Maximum tolerable outage (MTO)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

An information security manager has been made aware of a new data protection regulation that will soon go into effect. Which of the following is the BEST way to manage the risk of noncompliance?

- A. Understand the cost of noncompliance.
- B. Implement a program of work to comply with the new legislation.
- C. Consult with senior management on the best course of action.
- D. Perform a gap analysis.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

Management of a financial institution accepted an operational risk that consequently led to the temporary deactivation to a critical monitoring process. Which of the following should be the information security manager's GREATEST concern with this situation?

- A. Impact on compliance risk.
- B. Inability to determine short-term impact.
- C. Impact on the risk culture.
- D. Deviation from risk management best practices

Answer: C ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation = The impact on the risk culture is the greatest concern for the information security manager, because it reflects the attitude and behavior of the organization towards risk management. If management accepts an operational risk that compromises a critical monitoring process, it may indicate a lack of awareness, commitment, or accountability for risk management. This may erode the trust and confidence of the stakeholders, regulators, and customers, and expose the organization to further risks. The impact on compliance risk, the inability to determine short-term impact, and the deviation from risk management best practices are also important, but they are secondary to the impact on the risk culture.

References = CISM Review Manual 15th Edition, page 48. CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question ID 421.

NEW QUESTION: 57

An information security manager is assessing security risk associated with a cloud service provider. Which of the following is the MOST appropriate reference to consult when performing this assessment?

- A. Previous provider service level agreements (SLAs)
- B. Security control frameworks
- C. Threat intelligence reports
- D. Penetration test results from the provider

Answer: ([SHOW ANSWER](#))

Security control frameworks (e.g., ISO/IEC 27001, NIST SP 800-53, CSA Cloud Controls Matrix) provide a structured and standardized approach to assess the security posture of cloud providers. These frameworks ensure completeness and alignment with best practices.

"Standardized security frameworks enable consistent evaluation of third-party providers and alignment with industry-recognized security requirements."

- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management* Penetration test results and SLAs are useful, but only frameworks provide comprehensive coverage.

NEW QUESTION: 58

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: ([SHOW ANSWER](#))

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/>

NEW QUESTION: 59

Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

- A. Review access permissions annually or whenever job responsibilities change
- B. Lock out accounts after a set number of unsuccessful login attempts.
- C. Delegate the management of access permissions to an independent third party.
- D. Enable multi-factor authentication on user and admin accounts.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 60

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: 61

An information security team has started work to mitigate findings from a recent penetration test. Which of the following presents the GREATEST risk to the organization?

- A. Some findings were reclassified to low risk after evaluation
- B. Not all findings from the penetration test report were fixed
- C. The penetration testing report did not contain any high-risk findings

D. Risk classification of penetration test findings was not performed

Answer: ([SHOW ANSWER](#))

The greatest risk comes from not performing risk classification on the findings. Without classification, the organization cannot prioritize remediation efforts, allocate resources effectively, or understand the business impact of the vulnerabilities.

"Risk classification helps determine the priority for mitigating vulnerabilities and enables risk-informed decisions."

- CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Analysis* Even if some findings are unfixed or reclassified, the lack of any classification process undermines the whole risk management effort.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: [freecram](#))

NEW QUESTION: 62

Which of the following BEST facilitates the effectiveness of cybersecurity incident response?

- A.** Utilizing a security information and event management (SIEM) tool.
- B.** Utilizing industry-leading network penetration testing tools.
- C.** Increasing communication with all incident response stakeholders.
- D.** Continuously updating signatures of the anti-malware solution.

Answer: ([SHOW ANSWER](#))

Communication is a key factor for the effectiveness of cybersecurity incident response, as it ensures that all relevant parties are informed, coordinated, and aligned on the incident status, impact, actions, and responsibilities. Communication also helps to maintain trust, confidence, and transparency among the stakeholders, such as senior management, business units, customers, regulators, law enforcement, and media. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.4.2.11

NEW QUESTION: 63

An information security manager has discovered a new technique that cybercriminals are exploiting. Which of the following has the manager identified?

- A.** A risk
- B.** A threat
- C.** An incident
- D.** An event

Answer: (SHOW ANSWER)

A new technique exploited by cybercriminals represents a threat (B). In CISM terminology, a threat is any circumstance or event with the potential to adversely impact an asset by exploiting a vulnerability. A risk (A) requires both a threat and a vulnerability with associated impact. An incident (C) is a realized event that compromises security, and an event (D) is an observable occurrence that may or may not lead to an incident.

Identifying new threat techniques is a key part of proactive risk management and threat intelligence activities emphasized in CISM.

References: ISACA CISM Review Manual (Risk management-threats, vulnerabilities, and risk definitions); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 64

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: 65

The PRIMARY advantage of performing black-box control tests as opposed to white-box control tests is that they:

- A. cause fewer potential production issues.
- B. require less IT staff preparation.
- C. simulate real-world attacks.
- D. identify more threats.

Answer: ([SHOW ANSWER](#))

The primary advantage of performing black-box control tests as opposed to white-box control tests is that they simulate real-world attacks. Black-box control tests are a software testing methodology in which the tester analyzes the functionality of an application without a thorough knowledge of its internal design. Conversely, in white-box control tests, the tester is knowledgeable of the internal design of the application and analyzes it during testing. By performing black-box control tests, the tester can mimic the perspective and behavior of an external attacker who does not have access to the source code or the implementation details of the application.

This way, the tester can evaluate how the application responds to different inputs and scenarios, and identify any vulnerabilities or errors that may affect its functionality or security. The other options are not the primary advantage of performing black-box control tests, although they may be some benefits or drawbacks depending on the context. Causing fewer potential production issues is not necessarily true, as black-box control tests may still introduce errors or disruptions to the application if not performed carefully. Requiring less IT staff preparation is not always true, as black-box control tests may still require a lot of planning and documentation to ensure adequate test coverage and quality. Identifying more threats is not necessarily true, as black-box control tests may miss some threats that are hidden in the internal logic or structure of the application.

NEW QUESTION: 66

Information security needs to invest in new tools to align with a recently updated bring your own device (BYOD) policy that now includes wearable technologies. Which of the following would BEST demonstrate return on investment (ROI) in risk management when presenting to the strategy committee for review?

- A. Business case
- B. Risk assessment
- C. Risk audit report
- D. Business impact analysis (BIA)

Answer: ([SHOW ANSWER](#))

A business case best demonstrates return on investment in risk management when requesting investment in new tools. In CISM, a business case connects the proposed investment to business objectives, risk reduction, cost, benefits, alternatives, and expected value. For a BYOD policy expanded to include wearable technologies, management needs to understand why new tools are required, what risks they reduce, what costs are involved, and how the investment supports acceptable risk levels. A risk assessment is an important input because it identifies and analyzes risks associated with wearable technologies, but it does not itself demonstrate ROI. A risk audit report provides assurance or findings, not the investment justification. A BIA supports continuity planning and impact prioritization, but it is not the best document for presenting investment value. The strategy committee needs a decision-oriented justification. Therefore, the business case is the best answer because it translates security needs and risk reduction into management-level investment rationale.

References:

ISACA CISM Review Manual , Information Security Program Development and Management - business cases and security investment justification ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 67

Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?

- A. Forensics certification
- B. Tabletop exercises
- C. Disaster recovery drills
- D. Penetration tests

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 68

A financial institution is planning to develop a new mobile application. Which of the following is the BEST time to begin assessments of the application's security compliance?

- A. During regulatory review
- B. During the design phase
- C. During static code analysis
- D. During user acceptance testing (UAT)

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 69

Which of the following groups is MOST important to involve in the development of information security procedures?

- A. Audit management
- B. Senior management
- C. Operational units
- D. End users

Answer: C ([LEAVE A REPLY](#))

The correct answer is C because procedures describe specific operational steps for carrying out security requirements, and operational units are the groups that must execute those steps in practice. Procedures must be realistic, workable, and aligned with day-to-day business and technical processes. Involving operational units helps ensure that procedures reflect actual workflows, system dependencies, resource constraints, and control responsibilities. Audit management may review procedures for compliance or control adequacy, but auditors should not be the primary developers of operational procedures. Senior management approves direction and policy, but it usually does not define detailed procedural steps. End users may provide useful feedback for procedures affecting them, but operational units have the strongest understanding of how processes are performed and controlled. In CISM, effective security program management

requires translating policies and standards into practical procedures that can be implemented consistently. Therefore, operational units are the most important group to involve in procedure development.

Reference: CISM Information Security Program Development and Management; procedures, operational control implementation, policy hierarchy, and process ownership principles.

NEW QUESTION: 70

Which of the following should be the NEXT step after a security incident has been reported?

- A. Investigation
- B. Recovery
- C. Containment
- D. Escalation

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 71

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: 72

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: 73

Which of the following is MOST important in increasing the effectiveness of incident responders?

- A. Communicating with the management team
- B. Integrating staff with the IT department
- C. Testing response scenarios
- D. Reviewing the incident response plan annually

Answer: (SHOW ANSWER)

= Testing response scenarios is the most important factor in increasing the effectiveness of incident responders, as it allows them to practice their skills, identify gaps and weaknesses, evaluate the adequacy and feasibility of the incident response plan, and improve their coordination and communication. Testing response scenarios can also help to enhance the confidence and readiness of the incident responders, as well as to measure their performance and compliance with the policies and procedures. Testing response scenarios can be done through various methods, such as tabletop exercises, simulations, drills, or full-scale exercises, depending on the scope, objectives, and complexity of the scenarios.

The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is

updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents.

However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions.

References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

NEW QUESTION: 74

Which of the following presents the GREATEST challenge when assessing the impact of emerging risk?

- A. Complexity of the emerging risk
- B. Insufficient data related to the emerging risk
- C. Outdated risk management strategy
- D. Lack of resources to perform risk assessments

Answer: ([SHOW ANSWER](#))

The greatest challenge in assessing emerging risk is insufficient data (B). Emerging risks, by definition, lack historical incidents, loss data, and proven impact metrics, making accurate assessment difficult. CISM emphasizes that uncertainty and data scarcity are inherent challenges in emerging risk management.

Complexity (A) and resource constraints (D) are common issues, but without sufficient data, even skilled analysts and mature processes struggle to estimate likelihood and impact. An outdated strategy (C) affects overall effectiveness but does not specifically hinder impact assessment as much as data scarcity does.

References: ISACA CISM Review Manual (Risk management-emerging risks, uncertainty, and assessment challenges); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 75

Which of the following is MOST important for an information security manager to consider when determining whether data should be stored?

- A. Data storage limitations
- B. Type and nature of data
- C. Data protection regulations
- D. Business requirements

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 76

Which of the following should be given the HIGHEST priority during an information security post-incident review?

- A. Documenting actions taken in sufficient detail
- B. Updating key risk indicators (KRIs)
- C. Evaluating the performance of incident response team members

D. Evaluating incident response effectiveness

Answer: (SHOW ANSWER)

An information security post-incident review is a process that aims to identify the root causes, impacts, lessons learned, and improvement actions of a security incident. The highest priority during a post-incident review should be evaluating the effectiveness of the incident response, which means assessing how well the incident response plan, procedures, roles, resources, and communication were executed and aligned with the business objectives and requirements. Evaluating the incident response effectiveness can help to identify the gaps, weaknesses, strengths, and opportunities for improvement in the incident response process and capabilities. Documenting actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are also important activities during a post-incident review, but they are not as critical as evaluating the incident response effectiveness, which can provide a holistic and strategic view of the incident response maturity and value.

References =

* ISACA, CISM Review Manual, 16th Edition, 2020, page 2411

* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2192 During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)

NEW QUESTION: 77

Which of the following metrics is MOST appropriate for evaluating the incident notification process?

- A. Average total cost of downtime per reported incident
- B. Elapsed time between response and resolution
- C. Average number of incidents per reporting period
- D. Elapsed time between detection, reporting, and response

Answer: D (LEAVE A REPLY)

Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.

References:

<https://www.atlassian.com/incident-management/kpis/common-metrics>

<https://securityscorecard.com/blog/how-to-use-incident-response-metrics/>

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

NEW QUESTION: 78

What should be the information security manager's FIRST step when updating an information security program?

- A. Review costs and benchmark them against industry norms
- B. Re-evaluate the organization's business expectations and objectives
- C. Identify program components that do not align with business objectives
- D. Interview business unit managers and key stakeholders

Answer: (SHOW ANSWER)

The first step when updating an information security program is to re-evaluate the organization's business expectations and objectives . CISM emphasizes that the information security program must be aligned with business goals, risk appetite, and enterprise priorities. Before identifying misaligned components or interviewing stakeholders, the security manager must first understand the current business direction and expectations that the program must support. Benchmarking costs against industry norms may be useful later, but cost comparison does not define the program's required direction. Identifying misaligned components is only possible after current business objectives are understood. Interviewing business unit managers and stakeholders is a method that may support re-evaluation, but the primary first step is determining what the organization expects the updated program to achieve. Business objectives may change due to digital transformation, mergers, regulatory shifts, new products, or changing threat conditions. Therefore, re- evaluating business expectations and objectives is the correct starting point for updating the program.

References:

ISACA CISM Review Manual , Information Security Governance - business alignment and security program direction ISACA CISM Exam Content Outline , Domain 2: Information Security Governance

NEW QUESTION: 79

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

- A. Establish performance metrics for the team
- B. Perform a post-incident review
- C. Implement a SIEM solution
- D. Perform a threat analysis

Answer: ([SHOW ANSWER](#))

Performing a post-incident review (also known as a lessons-learned session) is the best way to ensure similar incidents are identified and addressed more efficiently in the future. This review helps in understanding what went wrong, what went right, and how processes can be improved. The knowledge gained from the review can be incorporated into incident response plans and training.

"Post-incident reviews help determine root causes, assess the effectiveness of the response, and identify opportunities for improvement."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis Additionally, the ISACA CISM Practice Question Database emphasizes that post-incident reviews are essential for improving future response times and understanding patterns of threats.

NEW QUESTION: 80

Which of the following is the PRIMARY benefit achieved when an information security governance framework is aligned with corporate governance?

- A. Protection of business value and assets
- B. Identification of core business strategiesC, Easier entrance into new businesses and technologies
- C. Improved regulatory compliance posture

Answer: ([SHOW ANSWER](#))

Information security governance 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, and are effectively managed. By aligning information security governance with corporate governance, the organization can ensure that information security is integrated into the business processes and decision making, and that the information security risks and opportunities are properly identified, assessed, and addressed.

References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.1

NEW QUESTION: 81

Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?

- A. The risks are reported to the business unit's senior management
- B. The risks are escalated to the IT department for remediation
- C. The risks are communicated to the central risk function
- D. The risks are entered in the organization's risk register

Answer: ([SHOW ANSWER](#))

Recording risks in the risk register ensures visibility, accountability, and tracking. This formal documentation is essential for assigning ownership, determining treatment strategies, and ensuring ongoing governance.

A risk that is not entered into the register may go unaddressed. This step supports structured risk tracking and compliance with governance practices.

"The risk register is the primary tool used to track, prioritize, assign, and monitor risks and their treatment. It forms the basis of a structured risk management program."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Documentation and Communication*

NEW QUESTION: 82

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

- A. rely on senior management to enforce security.
- B. promote the relevance and contribution of security.
- C. focus on compliance.
- D. reiterate the necessity of security.

Answer: ([SHOW ANSWER](#))

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security to the organization's goals and objectives. Security is not only a technical function, but also a business enabler that supports the organization's strategy, vision, and mission. By promoting the relevance and contribution of security, the information security manager can demonstrate the value and benefits of security to the stakeholders, such as increasing customer trust, enhancing reputation, reducing costs, improving efficiency, and complying with regulations. Promoting the relevance and contribution of security can also help the information security manager to build relationships and partnerships with the business units, and to align the security program with the business needs and expectations. Promoting the relevance and contribution of security can also help the information security manager to foster a positive security culture and awareness within the organization, and to encourage the adoption and support of security policies and practices.

The other options are not the best ways to overcome the perception that security is a hindrance to business activities. Relying on senior management to enforce security is not the best way, because it may create a sense of coercion and resentment among the employees, and may undermine the credibility and authority of the information security manager. Focusing on compliance is not the best way, because it may create a false sense of security and satisfaction, and may neglect the other aspects and dimensions of security, such as risk management, value

creation, and innovation. Reiterating the necessity of security is not the best way, because it may not address the root causes and factors of the negative perception, and may not provide sufficient evidence and justification for the security investments and decisions. References = CISM Review Manual,

16th Edition, ISACA, 2020, pp. 13-14, 23-241; CISM Online Review Course, Domain 1: Information Security Governance, Module 1: Information Security Governance Overview, ISACA2

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security. By demonstrating the value that security brings to the organization, including protecting assets and supporting business objectives, the information security manager can help to change the perception of security from a hindrance to a critical component of business success.

Relying on senior management to enforce security, focusing on compliance, and reiterating the necessity of security are all important elements of a comprehensive security program, but they do not directly address the perception that security is a hindrance to business activities. By promoting the relevance and contribution of security, the information security manager can help to align security with the overall goals and objectives of the organization, and foster a culture that values and supports security initiatives.

NEW QUESTION: 83

Which of the following should be an information security manager's FIRST course of action when a newly introduced privacy regulation affects the business?

- A. Consult with IT staff and assess the risk based on their recommendations
- B. Update the security policy based on the regulatory requirements
- C. Propose relevant controls to ensure the business complies with the regulation
- D. Identify and assess the risk in the context of business objectives

Answer: ([SHOW ANSWER](#))

Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

NEW QUESTION: 84

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. Centralized logging
- C. Available forensic tools
- D. Time clock synchronization

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 85

Following an unsuccessful denial of service (DoS) attack, identified weaknesses should be:

- A. Tracked and reported on until their final resolution
- B. Noted and re-examined later if similar weaknesses are found
- C. Documented in security awareness programs
- D. Quickly resolved and eliminated regardless of cost

Answer: ([SHOW ANSWER](#))

Any weaknesses identified, even after an unsuccessful attack, should be tracked and reported until they are fully resolved. This ensures accountability, remediation, and prevention of future incidents. Ignoring or delaying action increases exposure to future threats.

"All vulnerabilities must be tracked, assigned for remediation, and closed out following proper documentation and validation."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Remediation and Lessons Learned ISACA's guidance in the practice questions clearly recommends formal tracking and resolution of vulnerabilities as the best practice for ongoing security management.

NEW QUESTION: 86

Which of the following is the MOST important outcome of effective risk treatment?

- A. Elimination of risk
- B. Timely reporting of incidents
- C. Reduced cost of acquiring controls
- D. Implementation of corrective actions

Answer: ([SHOW ANSWER](#))

The most important outcome of effective risk treatment is the implementation of corrective actions that address the root causes of the risk and reduce its likelihood and/or impact to an acceptable level. Effective risk treatment does not necessarily eliminate the risk, but rather brings it within the organization's risk appetite and tolerance. Timely reporting of incidents and reduced cost of acquiring controls are desirable benefits of effective risk treatment, but they are not the primary outcome.

References: The CISM Review Manual 2023 defines risk treatment as "the process of selecting and implementing measures to modify risk" and states that "the objective of risk treatment is to implement corrective actions that will reduce the risk to a level that is acceptable to the enterprise" (p. 92). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Implementation of corrective actions is the correct answer because it is the most important outcome of effective risk treatment, as it ensures that the risk is managed in accordance with the organization's risk appetite and tolerance" (p. 28). Additionally, the Not All Risk Treatment Options Are the Same article from the ISACA Journal 2021 states that "risk treatment is the process of implementing corrective actions to address the root causes of the risk and to reduce the likelihood and/or impact of the risk" (p. 1)1.

NEW QUESTION: 87

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: 88

What is the BEST way to inform senior management of the value of information security?

- A. Present the benefits of security awareness training
- B. Describe how security enables business objectives
- C. Describe potential impact of compromises
- D. Present anticipated return on security investment

Answer: (SHOW ANSWER)

The most effective way to communicate the value of information security to senior management is to describe how security enables business objectives (B). CISM emphasizes that executives view security as valuable when it supports revenue generation, operational resilience, customer trust, and strategic goals. Discussing training benefits (A), potential impacts (C), or ROI (D) alone frames security as a cost or fear-based function.

Positioning security as a business enabler aligns it with executive priorities and promotes sustained support.

References: ISACA CISM Review Manual (Governance-executive communication and value realization); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 89

Which of the following BEST enables the design of an effective incident escalation process?

- A. Enforceable control baselines

- B. Controls designed for defense in depth
- C. A well-defined organizational hierarchy
- D. A comprehensive risk register

Answer: (SHOW ANSWER)

A well-defined organizational hierarchy best enables the design of an effective incident escalation process.

Incident escalation requires clarity about authority, reporting paths, decision-making responsibility, and communication channels. CISM incident management emphasizes that response processes must define roles, responsibilities, thresholds, and escalation procedures before incidents occur. Without a clear organizational hierarchy, incidents may be delayed, misrouted, or escalated to personnel without appropriate authority.

Enforceable control baselines and defense-in-depth controls are important for prevention and security consistency, but they do not define escalation paths. A comprehensive risk register supports risk management but does not by itself establish who must be notified or who can make response decisions during an incident.

Escalation must align with the organization's management structure so that operational, legal, communications, and executive decisions can be made quickly. Therefore, a well-defined organizational hierarchy is the strongest foundation for an effective escalation process.

References:

ISACA CISM Review Manual , Information Security Incident Management - escalation, roles, and responsibilities ISACA CISM Exam Content Outline , Domain 4: Information Security Incident Management

NEW QUESTION: 90

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

NEW QUESTION: 91

During a tabletop exercise, a security operations center team identifies a lack of resources to contain a security incident within an acceptable time frame. Which of the following is MOST likely to reduce containment time?

- A. Security orchestration, automation, and response
- B. Zero Trust Architecture
- C. Security information and event management
- D. Intrusion detection system

Answer: (SHOW ANSWER)

The correct answer is A because security orchestration, automation, and response directly reduces containment time by automating repetitive incident response actions. SOAR can automatically enrich alerts, open tickets, isolate endpoints, block malicious indicators, notify response teams, and execute predefined playbooks. In the scenario, the tabletop exercise identifies a resource constraint affecting timely containment.

The most appropriate solution is therefore a capability that improves response efficiency and reduces manual workload. Zero Trust Architecture is a broader security model based on continuous verification and least privilege, but it does not directly solve immediate containment resource limitations. SIEM is primarily used for log collection, correlation, detection, and alerting; it helps identify incidents but does not automatically contain them unless integrated with response automation. IDS detects suspicious activity but does not typically perform containment. From a CISM incident management perspective, response capability should support timely detection, escalation, containment, and recovery. SOAR is the best fit for reducing containment time. Reference: CISM Information Security Incident Management; incident response automation, containment, SOC operations, and response efficiency principles.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)

NEW QUESTION: 92

Which of the following BEST enables an organization to identify and contain security incidents?

- A. Risk assessments
- B. Threat modeling
- C. Continuous monitoring
- D. Tabletop exercises

Answer: (SHOW ANSWER)

= Continuous monitoring is the process of collecting, analyzing, and reporting on the security status of an organization's information systems and networks. Continuous monitoring enables an organization to identify and contain security incidents by providing timely and accurate information on the security events, alerts, incidents, and threats that may affect the organization. Continuous monitoring also helps to measure the effectiveness and compliance of the security controls, policies, and procedures that are implemented to protect the organization's information assets. Continuous monitoring can be performed using various tools and methods, such as security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), vulnerability scanners, log analyzers, and audit trails.

References = CISM Manual¹, Chapter 6: Incident Response Planning (IRP), Section 6.2: Continuous Monitoring²

1: <https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles> 2: 3

NEW QUESTION: 93

Which of the following is MOST important to the effectiveness of an information security steering committee?

- A. The committee has strong regulatory knowledge.
- B. The committee has cross-organizational representation.
- C. The committee is comprised of representatives from senior management.
- D. The committee uses a risk management framework.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 94

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).

NEW QUESTION: 95

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: 96

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: 97

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: C (LEAVE A REPLY)

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: 98

Which of the following is the FIRST step to establishing an effective information security program?

- A. Conduct a compliance review.
- B. Assign accountability.
- C. Perform a business impact analysis (BIA).
- D. Create a business case.

Answer: (SHOW ANSWER)

According to the CISM Review Manual, the first step to establishing an effective information security program is to create a business case that aligns the program objectives with the organization's goals and strategies. A business case provides the rationale and justification for the information security program and helps to secure the necessary resources and support from senior management and other stakeholders. A business case should include the following elements:

The scope and objectives of the information security program

The current state of information security in the organization and the gap analysis
The benefits and value proposition of the information security program
The risks and challenges of the information security program
The estimated costs and resources of the information security program
The expected outcomes and performance indicators of the information security program
The implementation plan and timeline of the information security program
References = CISM Review Manual, 16th Edition, Chapter 3, Section 2, pages 97-99.

NEW QUESTION: 99

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: 100

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

- A. Establish performance metrics for the team.
- B. Perform a post-incident review.
- C. Perform a threat analysis.
- D. Implement a SIEM solution.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 101

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

- A. Determine recovery priorities.
- B. Define the recovery point objective (RPO).
- C. Confirm control effectiveness.
- D. Analyze vulnerabilities.

Answer: ([SHOW ANSWER](#))

The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

NEW QUESTION: 102

Which of the following would BEST enable senior management to integrate security into all organizational processes following an increase in cyberattacks on business applications?

- A. Updating process diagrams to align with organizational strategy
- B. Requiring developers to attend customized training on secure application development
- C. Providing security training to key stakeholders within each business area
- D. Establishing security policies that align with business objectives

Answer: D ([LEAVE A REPLY](#))

The correct answer is D because senior management integrates security into organizational processes by establishing security policies that are aligned with business objectives. Policies communicate management's intent, define required behavior, and provide the foundation for standards, procedures, controls, and accountability across the enterprise. When policies align with business objectives, security becomes part of how the organization operates rather than a separate technical activity. Updating process diagrams may help document processes, but documentation alone does not integrate security. Developer training is useful for application security, but it applies mainly to development teams and not all organizational processes. Training key stakeholders is valuable, but training alone does not establish mandatory enterprise-wide requirements.

CISM governance principles emphasize that information security must support business goals, be directed by senior management, and be embedded into organizational structures and processes. Therefore, establishing business-aligned security policies is the best mechanism for integrating security into all organizational processes.

Reference: CISM Information Security Governance; policy alignment, senior management direction, business integration, and governance principles.

NEW QUESTION: 103

Which of the following tools provides an incident response team with the GREATEST insight into insider threat activity across multiple systems?

- A. A security information and event management (SIEM) system
- B. An intrusion prevention system (IPS)
- C. A virtual private network (VPN) with multi-factor authentication (MFA)
- D. An identity and access management (IAM) system

Answer: ([SHOW ANSWER](#)**)**

A SIEM system is the best tool for providing an incident response team with the greatest insight into insider threat activity across multiple systems because it can collect, correlate, analyze, and report on security events and logs from various sources, such as network devices, servers, applications, and user activities. A SIEM system can also detect and alert on anomalous or suspicious behaviors, such as unauthorized access, data exfiltration, privilege escalation, or policy violations, that may indicate an insider threat. A SIEM system can also support forensic investigations and incident response actions by providing a centralized and comprehensive view of the security posture and incidents.

References: The CISM Review Manual 2023 defines SIEM as "a technology that provides real-time analysis of security alerts generated by network hardware and applications" and states that "SIEM systems can help identify insider threats by correlating user activity logs with other security events and detecting deviations from normal patterns" (p. 184). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A security information and event management (SIEM) system is the correct answer because it can provide the most insight into insider threat activity across multiple systems by collecting, correlating, analyzing, and reporting on security events and logs from various sources" (p. 95). Additionally, the Detecting and Identifying Insider Threats article from the CISA website states that

"threat detection and identification is the process by which persons who might present an insider threat risk due to their observable, concerning behaviors come to the attention of an organization or insider threat team.

Detecting and identifying potential insider threats requires both human and technological elements" and that

"technological elements include tools such as security information and event management (SIEM) systems, user and entity behavior analytics (UEBA) systems, and data loss prevention (DLP) systems, which can monitor, analyze, and alert on user activities and network events" (p. 1)¹.

NEW QUESTION: 104

Which of the following should an organization do FIRST when confronted with the transfer of personal data across borders?

- A.** Define policies and standards for data processing.
- B.** Implement applicable privacy principles
- C.** Assess local or regional regulations
- D.** Research cyber insurance policies

Answer: ([SHOW ANSWER](#))

Before transferring personal data across borders, an organization should first assess the local or regional regulations that apply to the data protection and privacy of the data subjects. This will help the organization to identify the legal requirements and risks involved in the data transfer, and to choose the appropriate tools and safeguards to ensure compliance and protection. For example, the organization may need to obtain consent from the data subjects, use adequacy decisions, standard contractual clauses, or other mechanisms to ensure an adequate level of

protection in the third country, or rely on specific derogations for certain situations. The other options are not the first steps to take, although they may be relevant at later stages of the data transfer process. References = Guide to the cross-border transfer of personal data in the GDPR New guidance issued by the EDPB on international transfers of personal data Requirements for transferring personal information across borders

NEW QUESTION: 105

Which of the following is the BEST way to address data availability concerns when outsourcing information security administration?

- A. Create contingency plans.
- B. Develop service level agreements (SLAs).
- C. Stipulate insurance requirements.
- D. Require nondisclosure agreements (NDAs).

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 106

Which of the following should be the PRIMARY objective of an information security governance framework?

- A. Provide a baseline for optimizing the security profile of the organization.
- B. Demonstrate senior management commitment.
- C. Demonstrate compliance with industry best practices to external stakeholders.
- D. Ensure that users comply with the organization's information security policies.

Answer: ([SHOW ANSWER](#))

According to the Certified Information Security Manager (CISM) Study Manual, "The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks." While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 60.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

Special Discount Code: **freecram**)

NEW QUESTION: 107

A global organization has outsourced security processes to a service provider by means of a global agreement.

What is the MOST efficient approach to meet country-specific regulatory requirements?

- A. Include binding corporate rules into the global agreement
- B. Set up a governance organization for each country
- C. Review the agreement for each country separately
- D. Set up companion agreements for each country

Answer: A ([LEAVE A REPLY](#))

Binding Corporate Rules (BCRs) are legally enforceable and approved data protection policies used to facilitate compliance across multiple jurisdictions. Incorporating BCRs into a global agreement enables the organization to efficiently manage regulatory obligations across countries. "Binding corporate rules offer a scalable and consistent mechanism to address cross-border compliance in global outsourcing agreements."

- CISM Review Manual 15th Edition, Chapter 1: Governance, Section: Cross-Border Data Protection Considerations* Creating separate agreements per country is inefficient and complex compared to centralized BCR-based governance.

NEW QUESTION: 108

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: 109

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: 110

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: 111

Which of the following is the MOST important consideration when developing an approach to effectively contain security incidents?

- A. Isolating systems impacted by incidents from the production environment
- B. Mitigating reputational damage that may affect business
- C. Minimizing financial losses that may result from outages
- D. Assigning senior management accountability for incident containment

Answer: ([SHOW ANSWER](#))

Isolating impacted systems (A) is the most critical consideration for effective incident containment because it directly limits spread, escalation, and additional damage. CISM incident management guidance prioritizes technical containment actions that preserve evidence and protect unaffected systems. Reputational (B) and financial (C) concerns are important but are outcomes of how well containment is executed. Assigning accountability (D) supports governance but does not directly contain an incident. Rapid isolation is essential to reduce overall impact and enable effective eradication and recovery.

References: ISACA CISM Review Manual (Incident management-containment strategies); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 112

Which of the following is the BEST approach for data owners to use when defining access privileges for users?

- A. Define access privileges based on user roles.
- B. Adopt user account settings recommended by the vendor.
- C. Perform a risk assessment of the users' access privileges.
- D. Implement an identity and access management (IDM) tool.

Answer: ([SHOW ANSWER](#))

This approach is the best because it ensures that users have the minimum level of access required to perform their job functions, which reduces the risk of unauthorized access or misuse of data. User roles are defined based on the business needs and responsibilities of the users, and they can be easily managed and audited.

References: The CISM Review Manual 2023 states that "the data owner is responsible for defining the access privileges for each user role" and that "the data owner should ensure that the principle of least privilege is applied to all users" (p. 82). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Defining access privileges based on user roles is the best approach because it allows the data owner to assign the minimum level of access required for each role and to review and update the roles periodically" (p. 23).

NEW QUESTION: 113

What should be the FIRST step when an Internet of Things (IoT) device in an organization's network is confirmed to have been hacked?

- A. Monitor the network.
- B. Perform forensic analysis.
- C. Disconnect the device from the network,
- D. Escalate to the incident response team

Answer: ([SHOW ANSWER](#))

= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures¹²³. References =

* 1: CISM Review Manual 15th Edition, page 2004

* 2: CISM Practice Quiz, question 1072

* 3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

NEW QUESTION: 114

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. Perform network penetration testing.
- D. Conduct periodic awareness training.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 115

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: 116

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: 117

Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?

- A. Reduction in the impact of security incidents
- B. Increase in the frequency of security incident escalations
- C. Decrease in the number of security incidents
- D. Increase in the number of reported security incidents

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 118

Which of the following is MOST important to ensure the alignment of an information security program with the organizational strategy?

- A. Adoption of an industry recognized framework
- B. Benchmarking against industry peers
- C. Approval from senior management
- D. Identification of business-specific risk factors

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 119

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. Initiate the incident response plan.
- B. Escalate the issue to senior management.
- C. Validate the scope and impact with the business process owner.
- D. Review and validate the rules within the DLP system.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 120

An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

- A. Integrate information security risk assessments into the procurement process.
- B. Provide regular information security training to the procurement team.
- C. Invite IT members into regular procurement team meetings to influence best practice.
- D. Enforce the right to audit in procurement contracts with SaaS vendors.

Answer: ([SHOW ANSWER](#))

The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization.

Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.

Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.

Inviting IT members into regular procurement team meetings to influence best practice is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.

Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts.

References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection:

Procurement and Vendor Management, Page 141-1421

NEW QUESTION: 121

Which of the following would be MOST important to include in communications to customers impacted by an information security incident?

- A. Details of the type of data exposed
- B. Identities of the attackers
- C. Costs of the incident to the organization
- D. Technical information related to the incident

Answer: A ([LEAVE A REPLY](#))

The most important information to include in communications to impacted customers is the details of the type of data exposed (A). From a CISM incident management and governance perspective, customer communications must focus on information that enables affected individuals to understand their personal risk and take appropriate protective actions. Knowing what type of data

was exposed (e.g., personal identifiers, financial data, credentials, health information) allows customers to assess potential impact, such as identity theft or fraud, and to take timely mitigation steps.

Identities of attackers (B) are often unknown, sensitive, or irrelevant to customers' immediate needs. Costs to the organization (C) are internal matters and do not help customers protect themselves. Technical details (D) may cause confusion, expose additional security information, or create legal and reputational risk without providing practical value to customers.

CISM emphasizes that incident communications should be clear, accurate, relevant, and audience-focused, while also supporting legal, regulatory, and privacy obligations.

Communicating the type of data exposed is central to transparency, trust, and compliance with breach notification requirements.

References:

ISACA CISM Review Manual, Information Security Incident Management - incident communication and stakeholder notification
ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 122

Senior management recently approved a mobile access policy that conflicts with industry best practices.

Which of the following is the information security manager's BEST course of action when developing security standards for mobile access to the organization's network?

- A.** Align the standards with the organizational policy.
- B.** Align the standards with industry best practices.
- C.** Resolve the discrepancy before developing the standards.
- D.** Perform a cost-benefit analysis of aligning the standards to policy.

Answer: ([SHOW ANSWER](#))

The Information Security Manager's primary responsibility is to ensure that the organization's information assets are adequately protected. In this scenario, there is a conflict between the approved mobile access policy and industry best practices. Developing security standards based on a flawed policy could lead to significant security vulnerabilities.

Why the other options are not the best course of action:

- A). Align the standards with the organizational policy: This would perpetuate the misalignment with best practices, potentially leaving the organization exposed to risks.
- B). Align the standards with industry best practices: While this is ideal from a security perspective, it directly contradicts the approved policy, which could create operational and compliance issues.
- D). Perform a cost-benefit analysis of aligning the standards to policy: A cost-benefit analysis might be useful at some point, but it does not address the fundamental issue of a policy that is not in line with best practices.

Key CISM Principles Reflected:

Alignment with Organizational Objectives: Security standards and policies should support and enable the organization's business objectives.

Risk Management: Identifying, assessing, and mitigating risks are essential elements of information security management.

Governance: Effective governance ensures that information security activities are aligned with the organization's strategies and objectives.

In summary: The Information Security Manager should proactively engage senior management to highlight the discrepancy between the approved policy and industry best practices. The goal is to revise the policy to ensure it adequately addresses security risks while supporting the organization's objectives. Once the policy is aligned with best practices, the security standards can be developed accordingly.

NEW QUESTION: 123

Which of the following is the PRIMARY reason to perform a business impact analysis (BIA)?

- A. Determining risk mitigation options
- B. Prioritizing critical processes
- C. Establishing recovery point objectives (RPOs)
- D. Determining information sensitivity

Answer: B (LEAVE A REPLY)

The primary reason for performing a business impact analysis (BIA) is to prioritize critical business processes (B). In CISM, the BIA is a foundational activity for business continuity and resilience planning, designed to identify which business functions are most critical to organizational survival and must be restored first following a disruption. The BIA evaluates the impact of outages over time, enabling management to rank processes based on operational, financial, legal, and reputational consequences.

While establishing recovery point objectives (RPOs) (C) is an important output of the BIA, it is secondary to identifying and prioritizing critical processes. Determining risk mitigation options (A) is part of risk treatment, not the primary purpose of a BIA. Determining information sensitivity (D) relates to data classification, which is a separate governance activity.

CISM guidance clearly positions the BIA as a business-driven exercise that informs recovery priorities, recovery time objectives (RTOs), and continuity strategies. Without first prioritizing critical processes, recovery objectives and continuity planning cannot be effectively aligned with business needs.

References:

ISACA CISM Review Manual, Information Security Program Development and Management - Business Impact Analysis (BIA) objectives and outcomes ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 124

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: 125

Which of the following is the BEST way to build a risk-aware culture?

- A. Establish a channel for staff to report risks.
- B. Periodically test compliance with security controls.
- C. Ensure that threats are documented and communicated in a timely manner.
- D. Periodically change risk awareness messages.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 126

A proposal designed to gain buy-in from senior management for a new security project will be MOST effective if it includes:

- A. industry benchmarking gap analysis.
- B. projected return on investment (ROI).
- C. historical data of reported incidents.
- D. analysis of current threat landscape.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 127

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: 128

Which of the following risks is an example of risk transfer?

- A. Utilizing third-party applications
- B. Moving risk ownership to another department
- C. Conducting off-site backups
- D. Purchasing cybersecurity insurance

Answer: ([SHOW ANSWER](#))

Purchasing cybersecurity insurance is a textbook example of risk transfer - transferring financial risk to a third party (the insurer).

"Risk transfer shifts the impact of a risk to another party, such as through insurance or outsourcing."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*

NEW QUESTION: 129

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. Invoke the incident response plan.
- C. Activate the disaster recovery plan (DRP).
- D. Conduct security awareness training.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 130

Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?

- A. The security strategy is promoted.
- B. Fewer security incidents are reported.
- C. Security behavior is improved.
- D. More security incidents are detected.

Answer: ([SHOW ANSWER](#))

The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.

The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms. Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.

The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal, Volume 1, 2019, 1.

NEW QUESTION: 131

Which of the following should be the PRIMARY area of focus when mitigating security risks associated with emerging technologies?

- A.** Compatibility with legacy systems
- B.** Application of corporate hardening standards
- C.** Integration with existing access controls
- D.** Unknown vulnerabilities

Answer: (SHOW ANSWER)

= The primary area of focus when mitigating security risks associated with emerging technologies is unknown vulnerabilities. Emerging technologies are new and complex, and often involve multiple parties, interdependencies, and uncertainties. Therefore, they may have unknown vulnerabilities that could expose the organization to threats that are difficult to predict, detect, or prevent¹. Unknown vulnerabilities could also result from the lack of experience, knowledge, or best practices in implementing, operating, or securing emerging technologies². Unknown vulnerabilities could lead to serious consequences, such as data breaches, system failures, reputational damage, legal liabilities, or regulatory sanctions³. Therefore, it is important to focus on identifying, assessing, and addressing unknown vulnerabilities when mitigating security risks associated with emerging technologies.

The other options are not as important as unknown vulnerabilities, because they are either more predictable, manageable, or specific. Compatibility with legacy systems is a technical issue that could affect the performance, functionality, or reliability of emerging technologies, but it is not a security risk per se. It could be resolved by testing, upgrading, or replacing legacy systems⁴.

Application of corporate hardening standards is a security measure that could reduce the attack surface and improve the resilience of emerging technologies, but it is not a sufficient or comprehensive solution. It could be limited by the availability, applicability, or effectiveness of the standards. Integration with existing access controls is a security requirement that could prevent unauthorized or inappropriate access to emerging technologies, but it is not a guarantee of security. It could be challenged by the complexity, diversity, or dynamism of the access scenarios.

References = 1: Performing Risk Assessments of Emerging Technologies - ISACA 2: Assessing the Risk of Emerging Technology - ISACA 3: Factors Influencing Public Risk Perception of Emerging Technologies: A ... 4: CISM Review Manual 15th Edition, Chapter 3, Section 3.3 : CISM Review Manual

15th Edition, Chapter 3, Section 3.4 : CISM Review Manual 15th Edition, Chapter 3, Section 3.5

NEW QUESTION: 132

For which of the following is it MOST important that system administrators be restricted to read-only access?

- A. User access log files
- B. Administrator user profiles
- C. Administrator log files
- D. System logging options

Answer: ([SHOW ANSWER](#))

User access log files contain records of user activities and actions on the system, which can be used for auditing, monitoring, and investigating purposes. System administrators should not be able to modify or delete these files to ensure their integrity and availability. References = CISM Review Manual, 16th Edition, Chapter 3, Section 3.3.2.11

NEW QUESTION: 133

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: 134

Which of the following events would MOST likely require a revision to the information security program?

- A. An increase in industry threat level .
- B. A significant increase in reported incidents
- C. A change in IT management
- D. A merger with another organization

Answer: (SHOW ANSWER)

= A merger with another organization would MOST likely require a revision to the information security program, because it involves a significant change in the scope, structure, and objectives of the organization. A merger could affect the information security policies, procedures, roles, responsibilities, and resources of the organization, as well as introduce new risks and challenges. Therefore, the information security program should be reviewed and updated to reflect the new situation and ensure alignment with the organizational goals and strategies. An increase in industry threat level, a significant increase in reported incidents, and a change in IT management are all events that could affect the information security program without necessarily requiring a revision. References = CISM Review Manual, 16th Edition, page 3181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1532

NEW QUESTION: 135

The PRIMARY reason to create and externally store the disk hash value when performing forensic data acquisition from a hard disk is to:

- A. validate the confidentiality during analysis.
- B. reinstate original data when accidental changes occur.
- C. validate the integrity during analysis.
- D. provide backup in case of media failure.

Answer: (SHOW ANSWER)

The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD-ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital

evidence¹²³ References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532:

Guide to Computer Forensics and Investigations Fourth Edition, page 4-103:

Forensic disk acquisition over the network, Andrea Fortuna, 2018.

The main purpose of creating and storing an external disk hash value when performing forensic data acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

NEW QUESTION: 136

Which of the following BEST indicates the organizational benefit of an information security solution?

- A. Cost savings the solution brings to the information security department
- B. Reduced security training requirements
- C. Alignment to security threats and risks
- D. Costs and benefits of the solution calculated over time

Answer: (SHOW ANSWER)

The best option to indicate the organizational benefit of an information security solution is D. Costs and benefits of the solution calculated over time. This is because costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. ROSI can also help to justify the allocation and optimization of the resources and budget for the information security solution, and to compare and prioritize different security alternatives.

ROSI can be calculated by using various methods and formulas, such as the annualized loss expectancy (ALE), the annualized rate of occurrence (ARO), and the cost-benefit analysis (CBA). Costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.3, page 1311; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 99, page 26; How to Calculate Return on Security Investment (ROSI) - Infosec2

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 137

Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

- A. To compare emerging trends with the existing organizational security posture
- B. To communicate worst-case scenarios to senior management
- C. To train information security professionals to mitigate new threats

D. To determine opportunities for expanding organizational information security

Answer: A ([LEAVE A REPLY](#))

The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks.

References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

NEW QUESTION: 138

An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?

- A.** Identification of risk
- B.** Analysis of control gaps
- C.** Design of key risk indicators (KRIs)
- D.** Selection of risk treatment options

Answer: ([SHOW ANSWER](#)**)**

= Identification of risk is the first and most important step in the IT risk management process, especially when the organization is undergoing a digital transformation that introduces new technologies, processes, and business models. Identification of risk involves determining the sources, causes, and potential consequences of IT-related risks that may affect the organization's objectives, assets, and stakeholders. Identification of risk also helps to establish the risk context, scope, and criteria for the subsequent risk analysis, evaluation, and treatment. Without identifying the risks, the information security manager cannot effectively assess the risk exposure, prioritize the risks, implement appropriate controls, monitor the risk performance, or communicate the risk information to the relevant parties.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, page 841; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 34, page 352.

NEW QUESTION: 139

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: 140

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: (SHOW ANSWER)

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

NEW QUESTION: 141

Which of the following should be of GREATEST concern to an information security manager when evaluating a cloud service provider?

- A. Data retention policies are not documented
- B. There is no right to audit the security of the provider
- C. The provider is new to the market and lacks references
- D. Security controls offered by the provider are inadequate

Answer: (SHOW ANSWER)

The lack of audit rights prevents the organization from verifying the security posture and compliance of the provider, representing a major governance and assurance gap.

"Right to audit clauses ensure that organizations retain oversight and can verify the security controls and compliance of their service providers."

- CISM Review Manual 15th Edition, Chapter 3: Outsourced Services, Section: Third-Party Governance* Control inadequacy can be fixed; lack of oversight cannot be tolerated.

NEW QUESTION: 142

An organization implemented a number of technical and administrative controls to mitigate risk associated with ransomware. Which of the following is MOST important to present to senior management when reporting on the performance of this initiative?

- A. The total cost of the investment
- B. The cost and associated risk reduction
- C. The number and severity of ransomware incidents
- D. Benchmarks of industry peers impacted by ransomware

Answer: (SHOW ANSWER)

The most important information to present to senior management when reporting on the performance of the initiative to mitigate risk associated with ransomware is the cost and associated risk reduction, which means showing the value and effectiveness of the technical and administrative controls in terms of reducing the likelihood and impact of ransomware incidents and data extortion, and comparing them with the investment and resources required to implement and maintain them. The cost and associated risk reduction can help senior management to evaluate the return on investment (ROI) and the alignment with the business objectives and risk appetite of the initiative.

References = Ransomware Risk Management - NIST, #StopRansomware Guide | CISA

NEW QUESTION: 143

Which of the following is necessary to ensure consistent protection for an organization's information assets?

- A. Classification model
- B. Control assessment
- C. Data ownership
- D. Regulatory requirements

Answer: ([SHOW ANSWER](#))

The answer to the question is A. Classification model. This is because a classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by:

Providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets
Enabling the identification and prioritization of the information assets that need the most protection and resources
Facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification
Supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA)
A classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets, enabling the identification and prioritization of the information assets that need the most protection and resources, facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification, and supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets. (From CISM Manual or related resources)

References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISA Domain 5 - Protection of Information Assets²; CISM domain 3: Information security program development and management [2022 update]³; CISM Domain 2: Information Risk Management (IRM) [2022 update]⁴

NEW QUESTION: 144

Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

- A. perform testing to compare control performance against industry levels.
- B. ensure the controls are regularly tested for ongoing effectiveness.
- C. prepare to adapt the controls for future system upgrades.
- D. hand over the controls to the relevant business owners.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 145

Which of the following will BEST facilitate integrating the information security program into corporate governance?

- A. Documentation of the threat landscape
- B. An up-to-date security strategy
- C. A minimum security baseline
- D. Documentation of residual risk

Answer: ([SHOW ANSWER](#))

Documentation of residual risk (D) best facilitates the integration of the information security program into corporate governance because it directly supports executive decision-making and accountability, which are core elements of governance in CISM. Corporate governance requires senior management and the board to understand, evaluate, and formally accept risk in alignment with business objectives and risk appetite.

Residual risk documentation clearly communicates what risk remains after controls are applied and whether that risk is within acceptable tolerance.

While documentation of the threat landscape (A), an up-to-date security strategy (B), and a minimum security baseline (C) are all important program components, they primarily support operational security management, not governance integration. Governance focuses on oversight, transparency, and risk ownership, all of which are enabled when residual risk is documented, reported, and escalated appropriately.

CISM emphasizes that integrating security into corporate governance requires framing security outcomes in business risk terms that executives can act upon. Residual risk documentation provides the mechanism for informed risk acceptance, prioritization of investments, and alignment with enterprise risk management.

References:

ISACA CISM Review Manual, Information Security Governance - risk reporting, residual risk, and governance integration ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 146

When collecting admissible evidence, which of the following is the MOST important requirement?

- A. Need to know
- B. Preserving audit logs
- C. Due diligence
- D. Chain of custody

Answer: ([SHOW ANSWER](#))

Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved.

Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. References = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492 The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

NEW QUESTION: 147

Which of the following BEST helps to ensure risk appetite is considered during the risk treatment process?

- A. Formalized risk management framework
- B. Organization-wide risk awareness and training programs
- C. Use of a quantitative risk measurement approach
- D. Automated monitoring of key risk indicators (KRIs)

Answer: (SHOW ANSWER)

A formalized risk management framework (A) best ensures that risk appetite and risk tolerance are consistently applied during risk treatment decisions (mitigate, transfer, avoid, accept). In CISM risk management, risk appetite must be translated into decision criteria, escalation thresholds, approval authorities, and consistent evaluation methods—all of which are defined and enforced through a framework. Training and awareness (B) support culture, but they do not guarantee that treatment choices align with appetite in a repeatable, auditable way. Quantitative measurement (C) can improve precision, but even strong numbers can be misused without governance rules that tie outcomes to appetite thresholds and approval requirements. Automated KRI monitoring (D) helps track risk conditions, but it primarily supports ongoing monitoring, not the structured decision-making needed in treatment selection. A risk framework is the mechanism that institutionalizes appetite into processes, roles, reporting, and acceptance criteria.

References: ISACA CISM Review Manual (Risk management—risk appetite/tolerance, risk response, governance and oversight); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 148

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: B ([LEAVE A REPLY](#))

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: 149

Management would like to understand the risk associated with engaging an Infrastructure-as-a-Service (IaaS) provider compared to hosting internally. Which of the following would provide the BEST method of comparing risk scenarios?

- A. Mapping risk scenarios according to sensitivity of data
- B. Reviewing mitigating and compensating controls for each risk scenario
- C. Mapping the risk scenarios by likelihood and impact on a chart
- D. Performing a risk assessment on the IaaS provider

Answer: ([SHOW ANSWER](#))

Mapping the risk scenarios by likelihood and impact on a chart is the best method of comparing risk scenarios, as it helps to visualize and prioritize the different types and levels of risks associated with each option. A chart can also facilitate the communication and decision-making process by showing the trade-offs and benefits of each option. A chart can be based on qualitative or quantitative data, depending on the availability and accuracy of the information.

References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; A risk assessment model for selecting cloud service providers; Security best practices for IaaS workloads in Azure

NEW QUESTION: 150

What is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

- A. To share responsibility for addressing security breaches
- B. To gain acceptance of the policy across the organization
- C. To decrease the workload of the IT department
- D. To reduce the overall cost of policy development

Answer: ([SHOW ANSWER](#))

Involving stakeholders from various business units promotes buy-in, relevance, and adherence. When users feel they've had input in shaping the policy, they're more likely to support and follow it.

Stakeholders also provide insights into business processes that help ensure policies are practical and tailored.

This collaboration enhances organizational alignment and ensures policies do not create unintended operational friction.

"Stakeholder involvement is key to ensuring that policies are practical, aligned with operations, and accepted throughout the organization."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Policy Development and Implementation*

NEW QUESTION: 151

Which of the following BEST supports effective and timely incident response?

- A. Involving internal and external stakeholders
- B. Having a documented incident response plan in place
- C. Appointing a forensic incident response specialist
- D. Maintaining a SIEM solution

Answer: B ([LEAVE A REPLY](#))

The correct answer is B because a documented incident response plan provides the structured guidance needed for effective and timely response. The plan defines roles, responsibilities, escalation paths, communication procedures, severity classifications, containment strategies, evidence handling, notification requirements, and recovery coordination. Without a documented plan, response activities may be delayed, inconsistent, duplicated, or incomplete. Involving internal and external stakeholders is important, but stakeholder involvement must be organized through the incident response plan. Appointing a forensic specialist may be necessary for certain investigations, but not every incident requires forensic expertise. A SIEM solution is useful for monitoring and detection, but technology alone does not ensure that people know how to respond. CISM incident management principles emphasize preparation, documented procedures, communication, role clarity, and repeatable response processes. A documented plan enables responders to act quickly and consistently under pressure. Therefore, having a documented incident response plan in place best supports effective and timely incident response.

Reference: CISM Information Security Incident Management; incident response planning, documentation, escalation, communication, and response readiness principles.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 152

Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?

- A. The application does not use a secure communications protocol
- B. The application is configured with restrictive access controls
- C. The business process has only one level of error checking
- D. Server-based malware protection is not enforced

Answer: (SHOW ANSWER)

Server-based malware protection is not enforced is the issue that would be of GREATEST concern to an information security manager, as it exposes the web-based application and its data to potential threats from malicious software that can compromise the confidentiality, integrity, and availability of the information.

Server-based malware protection is a security control that monitors and blocks malicious activities on the server where the application runs, such as viruses, worms, trojans, ransomware, etc.

Without server-based malware protection, the web-based application may be vulnerable to attacks that can damage or destroy the data stored on the server, or disrupt the normal functioning of the application. The other issues are also important, but not as critical as server-based malware protection. The application does not use a secure communications protocol may expose sensitive data in transit to eavesdropping or interception by unauthorized parties. The application is configured with restrictive access controls may limit the access rights of legitimate users to authorized resources, but it does not prevent unauthorized users from accessing them through other means. The business process has only one level of error checking may result in incorrect or inconsistent data entry or processing, but it does not guarantee data quality or accuracy. References = CISM Review Manual, 16th Edition, page 1751; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 812

NEW QUESTION: 153

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: 154

Of the following, who is accountable for data loss in the event of an information security incident at a third- party provider?

- A. The information security manager
- B. The service provider that hosts the data
- C. The incident response team
- D. The business data owner

Answer: ([SHOW ANSWER](#))

The business data owner is accountable for data loss in the event of an information security incident at a third- party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third- party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan.

References: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud> <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned>

NEW QUESTION: 155

Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

- A. Management's business goals and objectives
- B. Strategies of other non-regulated companies
- C. Risk assessment results
- D. Industry best practices and control recommendations

Answer: A ([LEAVE A REPLY](#))

When a new information security manager is developing an information security strategy for a non-regulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

NEW QUESTION: 156

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: 157

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: 158

Which of the following should an information security manager do FIRST when creating an organization's disaster recovery plan (DRP)?

- A. Conduct a business impact analysis (BIA)
- B. Identify the response and recovery learns.
- C. Review the communications plan.
- D. Develop response and recovery strategies.

Answer: (SHOW ANSWER)

Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)². Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate solutions and procedures for restoring the critical business functions or processes.

References: 2 <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business-impact-analysis-bia-and-disaster-recovery-planning-drp>

NEW QUESTION: 159

When conducting a post-implementation review for a security investment, it is MOST important to determine whether the investment:

- A. Meets internal requirements
- B. Complies with industry standards
- C. Achieves projected financial benefits
- D. Delivers anticipated risk reduction

Answer: ([SHOW ANSWER](#))

The most important measure of a security investment's success is whether it delivers the anticipated risk reduction (D). CISM emphasizes that security investments are justified primarily by their ability to lower risk to within acceptable tolerance, not by compliance or financial return alone. Internal requirements (A) and standards compliance (B) are important but do not guarantee risk reduction. Financial benefits (C) are often indirect in security. Post-implementation reviews should validate whether the original risk assumptions were correct and whether residual risk aligns with management expectations.

References: ISACA CISM Review Manual (Program management-investment evaluation, risk-based performance measurement); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 160

Which of the following would be MOST helpful when creating information security policies?

- A. The information security framework
- B. Business impact analysis (BIA)
- C. Information security metrics
- D. Risk assessment results

Answer: ([SHOW ANSWER](#))

The information security framework is a set of principles, standards, guidelines, and best practices that define the scope, objectives, and requirements for information security in an organization. The information security framework is most helpful when creating information security policies because it provides a consistent and coherent approach to managing information security risks, aligning with business goals and strategy, and complying with relevant laws and regulations. The information security framework also helps to establish the roles, responsibilities, and accountability of all stakeholders involved in information security governance, management, and operations.

References = CISM Manual¹, Chapter 3: Information Security Program Development (ISPD), Section 3.1:

Information Security Framework²

1: <https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles> 2: 1

NEW QUESTION: 161

Who has the PRIMARY authority to decide if additional risk treatments are required to mitigate an identified risk?

- A. Information security manager

- B. IT risk manager
- C. Internal auditor
- D. Risk owner

Answer: ([SHOW ANSWER](#))

The risk owner is the person who has the authority and accountability to make decisions about the risk, including whether to accept, avoid, transfer, or mitigate it. The risk owner is also responsible for implementing and monitoring the risk treatment plan and reporting on the risk status. The risk owner is usually the business process owner or the information owner of the asset affected by the risk. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2.

NEW QUESTION: 162

Which of the following is MOST effective in gaining support for the information security strategy from senior management?

- A. Business impact analysis (BIA) results
- B. A major breach at a competitor
- C. Third-party security audit results
- D. Cost-benefit analysis results

Answer: ([SHOW ANSWER](#))

Senior management engagement is most effectively achieved when information security risks are clearly connected to real, tangible business consequences. A major breach at a competitor (B) provides a credible, industry-relevant example that demonstrates potential financial, operational, reputational, and regulatory impacts in a way executives readily understand. While BIA results (A), audit findings (C), and cost-benefit analyses (D) are important inputs, they are often abstract or internally focused. CISM guidance emphasizes that executive support is strongest when security messaging is business-driven, externally validated, and tied to strategic risk awareness. A peer breach highlights that the threat is realistic, imminent, and applicable to the organization's context, which increases urgency and executive buy-in for the security strategy.

References: ISACA CISM Review Manual (Governance-executive communication, stakeholder engagement); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 163

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: 164

Which of the following is MOST important to the effectiveness of an information security program?

- A. Security metrics
- B. Organizational culture
- C. IT governance
- D. Risk management

Answer: ([SHOW ANSWER](#))

Risk management is the most important factor for the effectiveness of an information security program, as it provides a systematic and consistent approach to identify, assess, treat, and monitor the information security risks that could affect the organization's objectives. Risk management also helps to align the security program with the business strategy, prioritize the security initiatives and resources, and communicate the value of security to the stakeholders.

References = CISM Review Manual 2022, page 3071; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.1

NEW QUESTION: 165

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: ([SHOW ANSWER](#))

"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: 166

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).

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 167

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

- 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: 168

A penetration test against an organization's external web application shows several vulnerabilities. Which of the following presents the GREATEST concern?

- A. A rules of engagement form was not signed prior to the penetration test
- B. Vulnerabilities were not found by internal tests
- C. Vulnerabilities were caused by insufficient user acceptance testing (UAT)
- D. Exploit code for one of the vulnerabilities is publicly available

Answer: (SHOW ANSWER)

Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.

References:

<https://www.imperva.com/learn/application-security/penetration-testing/>

<https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web-application-for-vulnerabilities/>

NEW QUESTION: 169

A PRIMARY purpose of creating security policies is to:

- A. define allowable security boundaries.
- B. communicate management's security expectations.
- C. establish the way security tasks should be executed.
- D. implement management's security governance strategy.

Answer: (SHOW ANSWER)

A security policy is a formal statement of the rules and principles that govern the protection of information assets in an organization. A security policy defines the scope, objectives, roles and responsibilities, and standards of the information security program. A primary purpose of creating security policies is to implement management's security governance strategy, which is the framework that guides the direction and alignment of information security with the business goals and objectives. A security policy translates the management's vision and expectations into specific and measurable requirements and controls that can be implemented and enforced by the information security staff and other stakeholders. A security policy also helps to establish the accountability and authority of the information security function and to demonstrate the commitment and support of the senior management for the information security program.

References =

* CISM Review Manual 15th Edition, page 1631

* CISM 2020: IT Security Policies2

* CISM domain 1: Information security governance [Updated 2022]3

* What is CISM? - Digital Guardian4

NEW QUESTION: 170

Which of the following is the PRIMARY reason to assign a risk owner in an organization?

- A. To remediate residual risk
- B. To define responsibilities
- C. To ensure accountability
- D. To identify emerging risk

Answer: ([SHOW ANSWER](#))

The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.

References: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

NEW QUESTION: 171

A business continuity plan (BCP) should contain:

- A. criteria for activation.
- B. information about eradication activities.
- C. data restoration procedures.
- D. hardware and software inventories.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 172

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: C ([LEAVE A REPLY](#))

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/2018/volume-3/change-management-in-the-age-of-digital-transformation)

<https://www.isaca.org/resources/isaca-journal/issues/>

NEW QUESTION: 173

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?

- 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: 174

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. There may be liabilities and penalties in the event of a security breach.
- B. Data may be stored in unknown locations and may not be easily retrievable.

- C. Laws and regulations of the origin country may not be applicable.
- D. Labeling of data may help to ensure data is assigned to the correct cloud type.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 175

Spoofing should be prevented because it may be used to:

- A. gain illegal entry to a secure system by faking the sender's address,
- B. predict which way a program will branch when an option is presented
- C. assemble information, track traffic, and identify network vulnerabilities.
- D. capture information such as passwords traveling through the network

Answer: A ([LEAVE A REPLY](#))

Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or something else to deceive or manipulate the recipient or target. Spoofing can be applied to various communication channels, such as emails, websites, phone calls, IP addresses, or DNS servers. One of the common goals of spoofing is to gain unauthorized access to a secure system by faking the sender's address, such as an email address or an IP address. For example, an attacker may spoof an email address of a trusted person or organization and send a phishing email that contains a malicious link or attachment. If the recipient clicks on the link or opens the attachment, they may be redirected to a fake website that asks for their credentials or downloads malware onto their device. Alternatively, an attacker may spoof an IP address of a trusted source and send packets to a secure system that contains malicious code or commands. If the system accepts the packets as legitimate, it may execute the code or commands and compromise its security. Therefore, gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented.

References:

- * <https://www.kaspersky.com/resource-center/definitions/spoofing>
- * <https://www.cisa.gov/resources-tools/resources/business-case-security>
- * <https://www.avast.com/c-spoofing>

NEW QUESTION: 176

An internal audit has revealed that a number of information assets have been inappropriately classified. To correct the classifications, the remediation accountability should be assigned to:

- A. the business users.
- B. the information owners.
- C. the system administrators.
- D. senior management.

Answer: ([SHOW ANSWER](#))

The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for

handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities.

This will improve the efficiency, effectiveness, and consistency of the incident response process.

References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation²

NEW QUESTION: 177

The PRIMARY purpose of implementing information security governance metrics is to:

- A. assess operational and program metrics.
- B. measure alignment with best practices.
- C. guide security towards the desired state.
- D. refine control operations.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 178

Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

- A. Collect additional metrics.
- B. Perform a cost-benefit analysis.
- C. Submit funding request to senior management.
- D. Begin due diligence on the outsourcing company.

Answer: ([SHOW ANSWER](#))

The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:

Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements
Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities
Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics
Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process
Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions
A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis

should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.

References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

NEW QUESTION: 179

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 responsibilities of both parties, the security controls and measures to be implemented, the security 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 Externalities - 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: 180

Which of the following is the BEST strategy when determining an organization's approach to risk treatment?

- A. Implementing risk mitigation controls that are considered quick wins
- B. Prioritizing controls that directly mitigate the organization's most critical risks
- C. Advancing the maturity of existing controls based on risk tolerance
- D. Implementing a one-size-fits-all set of controls across all organizational units

Answer: ([SHOW ANSWER](#))

Risk treatment should be prioritized based on risk criticality. Addressing the most severe and likely risks first ensures that resources are focused where they can have the greatest impact. "Risk treatment efforts should focus on the most significant risks first, based on likelihood and impact."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options*

NEW QUESTION: 181

Which of the following factors has the GREATEST influence on the successful implementation of information security strategy goals?

- A. Regulatory requirements
- B. Compliance acceptance
- C. Management support
- D. Budgetary approval

Answer: ([SHOW ANSWER](#))

Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance¹. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with². Compliance acceptance is the degree to which the organization adheres to the information security policies and standards³. Budgetary approval is the process of allocating financial resources for the information security activities and

initiatives4. References: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

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

NEW QUESTION: 182

Which of the following is the MOST effective way to demonstrate improvement in security performance?

- A. Report the results of a security control self-assessment (CSA).
- B. Provide a summary of security project return on investments (ROIs).
- C. Present vulnerability testing results.
- D. Present trends in a validated metrics dashboard.

Answer: (SHOW ANSWER)

Presenting trends in a validated metrics dashboard is the most effective way to demonstrate improvement in security performance because CISM emphasizes measurement over time, not isolated point-in-time results. A metrics dashboard allows senior management to see whether controls are becoming more effective, risks are being reduced, and objectives are being met consistently. Control self-assessments (A) and vulnerability test results (C) provide snapshots but lack context and trend analysis. ROI summaries (B) focus on financial performance rather than security effectiveness. CISM stresses that meaningful metrics must be aligned to business objectives, risk appetite, and key risk indicators, and must be repeatable and validated. Trending metrics demonstrate maturity, continuous improvement, and governance effectiveness, which are critical elements of an effective information security program.

References: ISACA CISM Review Manual (Program management-metrics, monitoring, and reporting); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 183

The BEST way to identify the risk associated with a social engineering attack is to:

- A. monitor the intrusion detection system (IDS),
- B. review single sign-on (SSO) authentication logs.
- C. test user knowledge of information security practices.
- D. perform a business risk assessment of the email filtering system.

Answer: (SHOW ANSWER)

The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.

Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.

Reviewing single sign-on (SSO) authentication lags (B) is not a relevant way to identify the risk associated with a social engineering attack. SSO is a method of authentication that allows users to access multiple applications or systems with one set of credentials. Authentication lags are delays or failures in the authentication process that may affect the user experience or performance. However, authentication lags are not directly related to social engineering attacks, as they do not indicate the user's knowledge of information security practices, nor the attacker's attempts or success in compromising the user's credentials or access.

Performing a business risk assessment of the email filtering system (D) is also not a relevant way to identify the risk associated with a social engineering attack. An email filtering system is a system that scans, filters, and blocks incoming or outgoing emails based on predefined rules or criteria, such as spam, viruses, or phishing. A business risk assessment is a process that evaluates the potential threats, vulnerabilities, and impacts to the organization's business objectives, processes, and assets. However, performing a business risk assessment of the email filtering system does not address the risk associated with a social engineering attack, as it only focuses on the technical aspects and performance of the system, not the human factors and behavior of the users.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, Subsection: Threat Identification, page 87-881

NEW QUESTION: 184

An information security manager is reporting on open items from the risk register to senior management.

Which of the following is MOST important to communicate with regard to these risks?

- A.** Responsible entities
- B.** Key risk indicators (KRIS)

- C. Compensating controls
- D. Potential business impact

Answer: ([SHOW ANSWER](#))

The most important information to communicate with regard to the open items from the risk register to senior management is the potential business impact of these risks. The potential business impact is the estimated consequence or loss that the organization may suffer if the risk materializes or occurs. The potential business impact can be expressed in quantitative or qualitative terms, such as financial, operational, reputational, legal, or strategic impact.

Communicating the potential business impact of the open items from the risk register helps senior management to understand the severity and urgency of these risks, and to prioritize the risk response actions and resources accordingly. Communicating the potential business impact also helps senior management to align the risk management objectives and activities with the business objectives and strategies, and to ensure that the risk appetite and tolerance of the organization are respected and maintained.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Reporting, page 1012.

NEW QUESTION: 185

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: ([SHOW ANSWER](#))

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: 186

Which of the following BEST facilitates the effective execution of an incident response plan?

- A. The plan is based on risk assessment results.
- B. The response team is trained on the plan
- C. The plan is based on industry best practice.
- D. The incident response plan aligns with the IT disaster recovery plan (DRP).

Answer: (SHOW ANSWER)

The effective execution of an incident response plan depends largely on the competence and readiness of the response team, who are responsible for carrying out the tasks and activities defined in the plan. Therefore, the best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan, and that they are familiar with their roles, responsibilities, procedures, and tools. Training the response team on the plan will also help to improve their confidence, communication, coordination, and collaboration during an incident response. The other options are not the best ways to facilitate the effective execution of an incident response plan, although they may be important factors for developing or improving the plan. The plan should be based on risk assessment results and industry best practice, but these do not guarantee that the plan will be executed effectively. The incident response plan should align with the IT disaster recovery plan, but this does not ensure that the response team is prepared and capable of executing the plan. References = CISM Review Manual, 16th Edition, page 1031 The best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan. An incident response plan is a set of instructions that defines the roles, responsibilities, procedures, and tools for detecting, responding to, and recovering from security incidents. An incident response team is a group of individuals that are assigned to perform specific tasks and activities during an incident response process. The response team may include security analysts, IT staff, legal counsel, public relations, and other stakeholders. To execute an incident response plan effectively, the response team needs to be trained on the plan, which means they need to be familiar with the following aspects of the plan:

The scope and objectives of the plan
The roles and responsibilities of each team member
The communication and escalation protocols
The incident classification and prioritization criteria
The incident response procedures and tools
The incident documentation and reporting requirements
The incident review and improvement processes

By training the response team on the plan, the organization can ensure that the team members are prepared and confident to handle any security incidents that may occur, and that they can perform their tasks efficiently and consistently. The other options are not the best way to facilitate the effective execution of an incident response plan, although they may be some steps or outcomes of the process. The plan being based on risk assessment results is a desirable practice, as it ensures that the plan is aligned with the organization's risk profile and addresses the most relevant and likely threats and vulnerabilities.

However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The plan being based on industry best practice is a desirable practice, as it ensures that the plan follows established standards and guidelines for incident response. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The incident response plan aligning with the IT disaster recovery plan (DRP) is a desirable practice, as it ensures that the plans are consistent and coordinated in terms of objectives, scope, roles, procedures, and tools. However, it does not

guarantee that the plan will be executed effectively unless the response team is trained on the plan

NEW QUESTION: 187

Which of the following is the MAIN feature of a web application firewall?

- A.** Modifying its predefined configuration automatically based on malicious traffic
- B.** Restricting external traffic within a private network
- C.** Redirecting distributed denial-of-service attacks
- D.** Filtering incoming Hypertext Transfer Protocol traffic

Answer: ([SHOW ANSWER](#))

The correct answer is D because the primary function of a web application firewall is to inspect, filter, and block malicious HTTP and HTTPS traffic directed at web applications. A WAF is specifically designed to protect web applications from attacks such as SQL injection, cross-site scripting, malicious requests, and protocol abuse. It operates at the application layer and evaluates web requests and responses based on rules, signatures, behavior, and application-specific policies. Automatically modifying its configuration may be a feature of some advanced adaptive tools, but it is not the main defining feature of a WAF. Restricting external traffic within a private network is more closely related to network firewalls or segmentation controls.

Redirecting distributed denial-of-service attacks is usually handled by DDoS protection services, content delivery networks, or traffic scrubbing solutions. In CISM terms, the correct control must match the risk and technology layer being protected. Since a WAF protects web applications by filtering web traffic, option D is the best answer.

Reference: CISM Information Security Program Development and Management; technical security controls, application protection, and web application security principles.

NEW QUESTION: 188

Which of the following BEST facilitates recovery of data lost as a result of a cybersecurity incident?

- A.** Removable storage media
- B.** Disaster recovery plan (DRP)
- C.** Offsite data backups
- D.** Encrypted data drives

Answer: ([SHOW ANSWER](#))

The best option to facilitate recovery of data lost as a result of a cybersecurity incident is offsite data backups.

This is because offsite data backups provide a secure and reliable way to restore data that may have been corrupted, deleted, or encrypted by malicious actors. Offsite data backups also reduce the risk of data loss due to physical damage, theft, or natural disasters that may affect the primary data storage location. Offsite data backups should be part of a comprehensive disaster recovery plan (DRP) that defines the roles, responsibilities, procedures, and resources for restoring normal operations after a cyber incident.

NEW QUESTION: 189

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: 190

An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk?

- A. Requirement for regular information security awareness
- B. Right-to-audit clause
- C. Service level agreement (SLA)
- D. Requirement to comply with corporate security policy

Answer: (SHOW ANSWER)

The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The

requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.

References = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NEW QUESTION: 191

Which of the following methods is the BEST way to demonstrate that an information security program provides appropriate coverage?

- A.** Security risk analysis
- B.** Gap assessment
- C.** Maturity assessment
- D.** Vulnerability scan report

Answer: (SHOW ANSWER)

A gap assessment is the best way to demonstrate that an information security program provides appropriate coverage, as it compares the current state of the information security program with the desired state based on the organization's objectives, policies, standards, and regulations. A gap assessment can identify the strengths and weaknesses of the information security program, as well as the areas that need improvement or alignment.

A gap assessment can also provide recommendations and action plans to close the gaps and achieve the desired level of information security coverage.

The other options are not as good as a gap assessment, as they do not provide a comprehensive and holistic view of the information security coverage. Security risk analysis is a process to identify and evaluate the risks to the information assets and the impact of potential threats and vulnerabilities. It can help to prioritize and mitigate the risks, but it does not measure the compliance or performance of the information security program.

Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. 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 1015.

CISM domain 3: Information security program development and management [2022 update], Infosec Certifications, 2.

NEW QUESTION: 192

An organization has remediated a security flaw in a system. Which of the following should be done NEXT?

- A.** Assess the residual risk.

- B. Share lessons learned with the organization.
- C. Update the system's documentation.
- D. Allocate budget for penetration testing.

Answer: ([SHOW ANSWER](#))

Residual risk is the risk that remains after applying controls to mitigate the original risk. It is important to assess the residual risk after remediation to ensure that it is within the acceptable level and tolerance of the organization. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 193

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: 194

To ensure that a new application complies with information security policy, the BEST approach is to:

- A. review the security of the application before implementation.
- B. integrate functionality the development stage.
- C. perform a vulnerability analysis.
- D. periodically audit the security of the application.

Answer: (SHOW ANSWER)

Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment. References: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle>
<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions>

NEW QUESTION: 195

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: B (LEAVE A REPLY)

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: 196

A common drawback of email software packages that provide native encryption of messages is that the encryption:

- A. cannot encrypt attachments
- B. cannot interoperate across product domains.
- C. has an insufficient key length.
- D. has no key-recovery mechanism.

Answer: (SHOW ANSWER)

Email software packages that provide native encryption of messages use proprietary algorithms and formats that are not compatible with other email software packages. This means that the encryption cannot interoperate across product domains, and the recipients of encrypted messages must use the same email software package as the sender to decrypt and read the messages. This limits the usability and scalability of native encryption, and may also pose security risks if the encryption algorithms or formats are not well-tested or widely accepted. A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains¹²³⁴. References = CISM Review Manual 15th Edition, page 206. The Top 10 Email Encryption Solutions In 2023 - Expert Insights², The Best Email Encryption Services for 2023 | PCMag³, The Top 12 Email Encryption Services for 2023 - Right Inbox⁴.

A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 197

Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?

- A.** Low number of false positives
- B.** Low number of false negatives
- C.** High number of false positives
- D.** High number of false negatives

Answer: D ([LEAVE A REPLY](#))

A false negative is a security incident that was not detected by the SIEM system, which presents the greatest risk as it allows attackers to compromise the organization's assets and data without being noticed or stopped.

A high number of false negatives can indicate that the SIEM system is not configured properly, has insufficient data sources, or lacks effective analytics and correlation rules. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 198

A new regulatory requirement affecting an organization's information security program is released. Which of the following should be the information security manager's FIRST course of action?

- A. Perform a gap analysis.
- B. Conduct benchmarking.
- C. Notify the legal department.
- D. Determine the disruption to the business.

Answer: (SHOW ANSWER)

= A new regulatory requirement affecting an organization's information security program is released. The information security manager's first course of action should be to notify the legal department, as they are responsible for ensuring compliance with the relevant laws and regulations. The legal department can advise the information security manager on how to interpret and implement the new requirement, as well as what are the potential implications and risks for the organization¹².

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

1. [isaca.org](https://www.isaca.org) 2. [csoonline.com](https://www.csoonline.com)

NEW QUESTION: 199

Which of the following is the BEST way to monitor for advanced persistent threats (APT) in an organization?

- A. Network with peers in the industry to share information.
- B. Browse the Internet to learn of potential events
- C. Search for anomalies in the environment
- D. Search for threat signatures in the environment.

Answer: C (LEAVE A REPLY)

An advanced persistent threat (APT) is a stealthy and sophisticated attack that aims to compromise and maintain access to a target network or system over a long period of time, often for espionage or sabotage purposes. APTs are difficult to detect by conventional security tools, such as antivirus or firewalls, that rely on signatures or rules to identify threats. Therefore, the best way to monitor for APTs is to search for anomalies in the environment, such as unusual network traffic, user behavior, file activity, or system configuration changes, that may indicate a compromise or an ongoing attack. References: <https://www.isaca.org/credentialing/cism> <https://www.nist.gov/publications/information-security-handbook-guide-managers>

NEW QUESTION: 200

Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?

- A. The risks are entered in the organization's risk register.
- B. The risks are reported to the business unit's senior management.
- C. The risks are escalated to the IT department for remediation.
- D. The risks are communicated to the central risk function.

Answer: A ([LEAVE A REPLY](#))

Entering identified risks into the organization's risk register ensures that they are documented, tracked, assigned, and addressed. Without recording in the risk register, there's no formal mechanism to manage, treat, or monitor the risk.

"The risk register is the central repository for tracking all known risks, their status, and treatment plans."

- CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Risk Response and Risk Register*

NEW QUESTION: 201

Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?

- A. Conduct a risk assessment.
- B. Document disaster recovery procedures.
- C. Identify business requirements.
- D. Perform a business impact analysis (BIA).

Answer: ([SHOW ANSWER](#))

The business impact analysis (BIA) is the foundational step in disaster recovery planning. The CISM Review Manual states that BIA should be performed first to determine critical business functions, recovery priorities, and the impact of disruptions. Risk assessments and documentation follow after the BIA.

Reference: ISACA CISM Review Manual, 16th Edition, Page 237-238, "Business Impact Analysis (BIA) in DRP Development".

NEW QUESTION: 202

Which of the following has the GREATEST influence on an organization's information security strategy?

- A. The organization's risk tolerance
- B. The organizational structure
- C. Industry security standards
- D. Information security awareness

Answer: A ([LEAVE A REPLY](#))

An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy

should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives.

Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.

The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.

An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION: 203

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: 204

Which of the following would BEST mitigate accidental data loss events?

- A. Conduct periodic user awareness training.
- B. Obtain senior management support for the information security strategy.
- C. Conduct a data loss prevention (DLP) audit.
- D. Enforce a data hard drive encryption policy.

Answer: A ([LEAVE A REPLY](#))

Conducting periodic user awareness training is the best way to mitigate accidental data loss events because it can educate the users on the causes, consequences, and prevention of data

loss, and increase their awareness of the security policies and procedures of the organization. User awareness training can also help users to identify and report potential data loss incidents, and to adopt good practices such as backing up data, encrypting data, and using secure channels for data transmission and storage.

References: The article Mistakes Happen-Mitigating Unintentional Data Loss from the ISACA Journal 2018 states that "user awareness training is the most effective way to prevent unintentional data loss" and that "user awareness training should include information on the types and sources of data loss, the impact and cost of data loss, the legal and regulatory requirements for data protection, the organization's data security policies and procedures, the roles and responsibilities of users in data security, the best practices and tools for data security, and the reporting and escalation process for data loss incidents" (p. 2)¹. The Data Spill Management Guide from the Cyber.gov.au website also states that "user awareness training is an important preventative measure to reduce the likelihood of data spills" and that "user awareness training should cover topics such as data classification, data handling, data storage, data transmission, data disposal, and data spill reporting" (p. 2)

NEW QUESTION: 205

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: D ([LEAVE A REPLY](#))

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: 206

Senior management is concerned about data exposure through the use of public AI services.

Which of the following is the information security manager's BEST course of action?

- A.** Train all employees on the appropriate use of public AI services and confidential data.
- B.** Disable access to public AI from company devices.
- C.** Perform a business impact analysis (BIA) of public AI.
- D.** Perform a risk assessment of public AI with appropriate recommendations for senior management.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 207

The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:

- A. the internal audit manager.
- B. the information security officer.
- C. the steering committee.
- D. the board of directors.

Answer: ([SHOW ANSWER](#))

The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 208

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: 209

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

- A. Database server
- B. Proxy server
- C. Mail relay server
- D. Application server

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 210

In the context of DevSecOps, which of the following BEST enables the identification of vulnerabilities before software is released?

- A. Performing integration testing
- B. Testing executable code
- C. Automating code review
- D. Following secure coding standards

Answer: ([SHOW ANSWER](#))

The correct answer is C because automating code review enables vulnerabilities to be identified continuously and early in the DevSecOps pipeline before software is released. DevSecOps integrates security into development and operations through automation, collaboration, and continuous testing. Automated code review tools, including static application security testing, can scan source code for insecure coding patterns, injection flaws, hardcoded credentials, unsafe libraries, and other weaknesses before deployment. Integration testing is useful for verifying that components work together, but it may not identify many code-level security weaknesses. Testing executable code can help detect vulnerabilities later in the pipeline, but finding flaws after code is compiled or packaged may be less efficient than reviewing source code earlier. Secure coding standards are important, but standards alone do not identify vulnerabilities unless compliance is tested. CISM program management emphasizes embedding security into development processes and using controls that support early risk detection. Therefore, automated code review best enables vulnerability identification before release.

Reference: CISM Information Security Program Development and Management; DevSecOps, secure SDLC, automated security testing, code review, and vulnerability management principles.

NEW QUESTION: 211

Which of the following should be the PRIMARY goal of information security?

- A. Information management
- B. Regulatory compliance
- C. Data governance
- D. Business alignment

Answer: ([SHOW ANSWER](#))

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 212

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: B ([LEAVE A REPLY](#))

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: 213

Which of the following desired outcomes BEST supports a decision to invest in a new security initiative?

- A.** Enhanced security monitoring and reporting
- B.** Reduced control complexity
- C.** Enhanced threat detection capability
- D.** Reduction of organizational risk

Answer: ([SHOW ANSWER](#))

The reduction of organizational risk is the desired outcome that best supports a decision to invest in a new security initiative. The organizational risk is the level of exposure or uncertainty that the organization faces in achieving its objectives. The organizational risk is influenced by various factors, such as the threat landscape, the vulnerability of the assets, the impact of the incidents, and the effectiveness of the controls. The information security manager should evaluate the organizational risk and propose security initiatives that can reduce the risk to an acceptable level. The security initiatives should be aligned with the business goals, the risk appetite, and the available resources of the organization. The security initiatives should also provide a positive return on investment (ROI) or value for money (VFM) for the organization. The reduction of organizational risk is the ultimate goal and benefit of any security initiative, as it enhances the security posture, performance, and resilience of the organization. Enhanced security monitoring and reporting, reduced control complexity, and enhanced threat detection capability are all possible outcomes of security initiatives, but they are not the best ones to support a decision to invest in a new security initiative. These outcomes are more specific and technical, and they may not directly relate to the business objectives or the risk appetite of the organization. These outcomes are also intermediate or enabling, rather than final or ultimate, as they may not necessarily lead to the reduction of organizational risk. For example, enhanced security

monitoring and reporting may improve the visibility and awareness of the security status, but it may not prevent or mitigate the incidents. Reduced control complexity may simplify the security management and maintenance, but it may not address the emerging or evolving threats. Enhanced threat detection capability may increase the speed and accuracy of identifying the attacks, but it may not reduce the impact or the likelihood of the attacks. Therefore, the reduction of organizational risk is the best outcome to support a decision to invest in a new security initiative, as it demonstrates the value and effectiveness of the security initiative for the organization. References = CISM Review Manual 2023, page 40 1; CISM Practice Quiz 2

NEW QUESTION: 214

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: 215

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: 216

Which of the following teams is BEST suited to prepare a disaster recovery plan?

- A. Incident response
- B. Information technology
- C. Senior management
- D. Information security

Answer: B ([LEAVE A REPLY](#))

The correct answer is B because a disaster recovery plan focuses on restoring IT systems, infrastructure, applications, data, and technical services after a disruption. The information technology team is best suited to prepare the technical recovery procedures because it understands system dependencies, backup processes, infrastructure requirements, recovery sequences, technical configurations, and operational constraints. The incident response team handles security incidents and may coordinate with IT during recovery, but it is not usually responsible for preparing the full DRP. Senior management provides direction, funding, and approval, but does not create detailed technical recovery plans. The information security function provides requirements, risk input, and oversight, but disaster recovery planning is primarily an IT operational responsibility. CISM distinguishes between business continuity, disaster recovery, and incident response responsibilities. Because DRP is centered on restoration of IT services and systems, the IT team is best suited to prepare it.

Reference: CISM Information Security Incident Management; disaster recovery planning, IT recovery responsibilities, business continuity, and operational resilience principles.

NEW QUESTION: 217

An organization's information security manager reads on social media that a recently purchased vendor product has been compromised and customer data has been posted online. What should the information security manager do FIRST?

- A. Perform a business impact analysis (BIA).
- B. Notify local law enforcement agencies of a breach.
- C. Activate the incident response program.
- D. Validate the risk to the organization.

Answer: ([SHOW ANSWER](#)**)**

The first thing that the information security manager should do after reading about a vendor product compromise on social media is to validate the risk to the organization. This means

verifying the source and credibility of the information, determining if the organization uses the affected product, and assessing the potential impact and likelihood of the compromise on the organization's data and systems. Validating the risk to the organization will help the information security manager to decide on the appropriate course of action, such as activating the incident response program, notifying relevant stakeholders, or performing a BIA.

References: The CISM Review Manual 2023 states that "the information security manager is responsible for identifying and assessing the risks associated with the use of third-party products and services" and that "the information security manager should monitor and review the security performance and incidents of third-party products and services 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: "Validating the risk to the organization is the correct answer because it is the first and most important step to take after reading about a vendor product compromise on social media, as it will help the information security manager to confirm the accuracy and relevance of the information, and to evaluate the potential consequences and probability of the compromise on the organization's data and systems" (p. 63). Additionally, the article Defending Against Software Supply Chain Attacks from the CISA website states that "the first step in responding to a software supply chain attack is to validate the risk to the organization by verifying the source and credibility of the information, determining if the organization uses the affected software, and assessing the potential impact and likelihood of the compromise on the organization's data and systems" (p. 2)

NEW QUESTION: 218

Which of the following is the MOST important consideration during the design phase of a business impact analysis (BIA)?

- A. Selecting quality metrics to monitor business performance
- B. Estimating the likelihood that end-to-end processes will be disrupted
- C. Obtaining reserve funding to prepare for possible business failures
- D. Identifying critical functions for business operations

Answer: (SHOW ANSWER)

The design phase of a BIA must begin with identifying critical business functions, since they determine:

Which systems/processes need protection

Recovery priorities

Acceptable downtime (RTO/MTD)

Without clearly defining what 's critical, the BIA cannot guide resource allocation or continuity strategies effectively.

"A successful BIA must begin with identifying which business functions are critical to achieving organizational objectives."

- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery, Section: BIA Methodology*

NEW QUESTION: 219

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: 220

Which of the following is the BEST way to assess the risk associated with using a Software as a Service (SaaS) vendor?

- A. Verify that information security requirements are included in the contract.
- B. Request customer references from the vendor.
- C. Require vendors to complete information security questionnaires.
- D. Review the results of the vendor's independent control reports.

Answer: (SHOW ANSWER)

Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.

Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting those requirements.

The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.

Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment.

Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. References = CISM Review Manual 15th Edition, page 144 SaaS Security Risk and Challenges - ISACA1 SaaS Security Checklist & Assessment Questionnaire | LeanIX2 Risk Assessment Guide for Microsoft Cloud3

NEW QUESTION: 221

Which of the following activities is designed to handle a control failure that leads to a breach?

- A. Risk assessment
- B. Incident management
- C. Root cause analysis
- D. Vulnerability management

Answer: (SHOW ANSWER)

Incident management is the activity designed to handle a control failure that leads to a breach. Incident management is the process of identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. Incident management aims to minimize the impact of a breach, restore normal operations as quickly as possible, and prevent or reduce the likelihood of recurrence. Incident management involves several steps, such as:

Establishing an incident response team with clear roles and responsibilities
Developing and maintaining an incident response plan that defines the procedures, tools, and resources for handling incidents
Implementing detection and reporting mechanisms to identify and communicate incidents
Performing triage and analysis to assess the scope, severity, and root cause of incidents
Containing and eradicating the threat and preserving evidence for investigation and legal purposes
Recovering and restoring the affected systems and data to a secure state
Evaluating and improving the incident response process and controls based on lessons learned and best practices
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 223-232.

NEW QUESTION: 222

Which of the following is the PRIMARY preventive method to mitigate risks associated with privileged accounts?

- A. Provide privileged account access only to users who need it.
- B. Frequently monitor activities on privileged accounts.
- C. Perform periodic certification of access to privileged accounts.
- D. Eliminate privileged accounts.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 223

When developing a categorization method for security incidents, the categories **MUST**:

- A. align with industry standards.
- B. be created by the incident handler.
- C. have agreed-upon definitions.
- D. align with reporting requirements.

Answer: ([SHOW ANSWER](#))

When developing a categorization method for security incidents, the categories must have agreed-upon definitions. This means that the categories should be clear, consistent, and understandable for all the parties involved in the incident response process, such as the incident handlers, the stakeholders, the management, and the external authorities. Having agreed-upon definitions for the categories can help to ensure that the incidents are classified and reported accurately, that the appropriate actions and resources are allocated, and that the communication and coordination are effective. Aligning with industry standards, creating by the incident handler, and aligning with reporting requirements are not mandatory for developing a categorization method for security incidents, although they may be desirable or beneficial depending on the context and objectives of the organization. Aligning with industry standards can help to adopt best practices and benchmarks for incident response, but it may not be feasible or suitable for all types of incidents or organizations. Creating by the incident handler can allow for flexibility and customization of the categories, but it may also introduce inconsistency and ambiguity if the definitions are not shared or agreed upon by others. Aligning with reporting requirements can help to comply with legal or contractual obligations, but it may not cover all the aspects or dimensions of the incidents that need to be categorized. References = CISM Review Manual, 16th Edition, pages 200-2011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 822

When developing a categorization method for security incidents, the categories **MUST** have agreed-upon definitions. This is because having clear and consistent definitions for each category of incidents will help to ensure a common understanding and communication among the incident response team and other stakeholders. It will also facilitate the accurate and timely identification, classification, reporting and analysis of incidents. Having agreed-upon definitions will also help to avoid confusion, ambiguity and inconsistency in the incident management process

NEW QUESTION: 224

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

- A. Baselines

- B. Management objectives
- C. Best practices
- D. Maturity levels

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 225

Which of the following is the BEST evidence of alignment between corporate and information security governance?

- A. Security key performance indicators (KPIs)
- B. Project resource optimization
- C. Regular security policy reviews
- D. Senior management sponsorship

Answer: ([SHOW ANSWER](#))

Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the commitment and support of the top-level executives and board members for the information security program.

Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.

References =

CISM Review Manual 15th Edition, page 1631

CISM 2020: Information Security & Business Process Alignment, video 22

Certified Information Security Manager (CISM), page 33

NEW QUESTION: 226

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: B ([LEAVE A REPLY](#))

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.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 227

Which of the following is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider?

- A.** Obtain an independent audit report.
- B.** Require the provider to follow stringent data classification procedures.
- C.** Include high penalties for security breaches in the contract.
- D.** Review the provider's information security policies.

Answer: (SHOW ANSWER)

Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of the enterprise." Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers. One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

NEW QUESTION: 228

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: ([SHOW ANSWER](#))

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: 229

Which of the following should an information security manager do FIRST upon learning that a competitor has experienced a ransomware attack?

- A. Update indicators of compromise in the security systems.
- B. Review the current risk assessment.
- C. Conduct ransomware awareness training for all staff.
- D. Perform a full data backup.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 230

Which of the following is the BEST indication of a mature information security program?

- A. Security incidents are managed properly.
- B. Security spending is below budget.
- C. Security resources are optimized.
- D. Security audit findings are reduced.

Answer: ([SHOW ANSWER](#))

A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most

efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.

References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

NEW QUESTION: 231

Which of the following is the BEST way to reduce the risk associated with a bring your own device (BYOD) program?

- A. Implement a mobile device policy and standard.
- B. Implement a mobile device management (MDM) solution.
- C. Provide employee training on secure mobile device practices.
- D. Require employees to install an effective anti-malware app.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 232

Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

- A. Skills required for the incident response team
- B. A list of external resources to assist with incidents
- C. Service level agreements (SLAs)
- D. A detailed incident notification process

Answer: ([SHOW ANSWER](#))

A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right people are involved in the incident response, that the incident is handled in a timely and efficient manner, and that the relevant information is shared with the appropriate parties. Skills required for the incident response team, a list of external resources to assist with incidents, and service level agreements (SLAs) are also important elements of an incident response plan, but they are not as critical as the incident notification process. Skills required for the incident response team describe the competencies and qualifications of the team members, but they do not specify who should be notified or involved in the incident response. A list of external resources to assist with incidents provides a directory of external parties that can provide support or expertise in the incident response, but it does not define the criteria or process for engaging them. Service level agreements (SLAs) define the expectations and obligations of the service providers and the service recipients in the incident response, but they do not detail the steps or procedures for notifying or escalating incidents. References = CISM Review Manual, 16th Edition, pages 191-1921; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 662

NEW QUESTION: 233

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: 234

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: A ([LEAVE A REPLY](#))

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: 235

An organization has introduced a new bring your own device (BYOD) program. The security manager has determined that a small number of employees are utilizing free cloud storage services to store company data through their mobile devices. Which of the following is the MOST effective course of action?

- A. Allow the practice to continue temporarily for monitoring purposes.
- B. Disable the employees' remote access to company email and data
- C. Initiate remote wipe of the devices
- D. Assess the business need to provide a secure solution

Answer: (SHOW ANSWER)

The most effective course of action when employees are using free cloud storage services to store company data through their mobile devices is to assess the business need to provide a secure solution, such as a corporate-approved cloud service or a virtual desktop environment. Assessing the business need can help understand why employees are using free cloud storage services, what kind of data they are storing, and what are the security risks and requirements. Based on the assessment, the security manager can propose a secure solution that meets the business needs and complies with the BYOD policy. The other options, such as allowing the practice to continue, disabling remote access, or initiating remote wipe, may not address the underlying business need or may cause disruption or data loss. References:

* <https://www.digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach>

* <https://news.microsoft.com/en-xm/2021/03/18/how-to-have-secure-remote-working-with-a-byod-policy/>

* <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod>

NEW QUESTION: 236

Which type of policy BEST helps to ensure that all employees, contractors, and third-party users receive formal communication regarding an organization's security program?

- A. Management review policy
- B. Business continuity management policy
- C. Information security training policy
- D. Security incident management policy

Answer: ([SHOW ANSWER](#))

The information security training policy ensures that everyone within the organization, including contractors and third-party users, receives the appropriate level of security awareness and training. This policy defines how the organization communicates its security requirements, expectations, and best practices.

"Information security training policies and programs ensure that all personnel are aware of and understand the security requirements and their individual responsibilities."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training The ISACA CISM practice questions emphasize that a clear training policy is the best way to communicate security practices to all involved parties.

NEW QUESTION: 237

Which of the following is the FIRST step in developing a business continuity plan (BCP)?

- A. Identify the applications with the shortest recovery time objectives (RTOs).
- B. Determine the business recovery strategy.
- C. Identify critical business processes.
- D. Determine available resources.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 238

An organization has recently purchased cybersecurity insurance after the board voiced concern about the potential for a security breach. With this response to the perceived risk, the organization:

- A. Has avoided the risk associated with a security breach
- B. Can safely reduce its internal security expenditure
- C. Remains ultimately accountable for the impact of a breach
- D. Has implemented redundant controls against a breach

Answer: ([SHOW ANSWER](#))

Even with cybersecurity insurance, the organization remains ultimately accountable for the impact of a breach (C). Insurance represents risk transfer, not risk elimination or avoidance. CISM clearly states that accountability for risk cannot be transferred; only financial impact may be partially offset. Insurance does not justify reducing security controls (B) and does not constitute redundant controls (D). Avoidance (A) would require eliminating the risky activity entirely. Management must continue to manage, monitor, and mitigate risk in line with appetite, regardless of insurance coverage.

References: ISACA CISM Review Manual (Risk management-risk response strategies, risk transfer); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 239

Which of the following should an information security manager do FIRST after discovering that a business unit has implemented a newly purchased application and bypassed the change management process?

- A. Revise the procurement process.
- B. Update the change management process.
- C. Discuss the issue with senior leadership.
- D. Remove the application from production.

Answer: (SHOW ANSWER)

An information security manager should first discuss the issue with senior leadership to escalate the problem and seek their support and guidance. Bypassing the change management process can introduce significant risks to the organization, such as unauthorized access, data loss, system instability, or compliance violations.

The information security manager should explain the potential impact and consequences of the incident, and recommend corrective actions to remediate the situation. The information security manager should also review the root cause of the incident and identify any gaps or weaknesses in the existing policies, procedures, or controls that allowed the business unit to implement the new application without proper authorization, testing, or documentation. The information security manager should then revise the procurement process, update the change management process, or implement other measures to prevent similar incidents from occurring in the future. Removing the application from production may not be feasible or desirable, depending on the business needs and the severity of the risks involved. References = CISM Review Manual, 16th Edition, pages 100-1011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page

2692

Learn more:

1. isaca.org
2. amazon.com
3. gov.uk

NEW QUESTION: 240

The MOST important element in achieving executive commitment to an information security governance program is:

- A. a defined security framework.
- B. a process improvement model
- C. established security strategies.
- D. identified business drivers.

Answer: (SHOW ANSWER)

The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive

can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

NEW QUESTION: 241

Which of the following should be the MOST important consideration when establishing information security policies for an organization?

- A.** Job descriptions include requirements to read security policies.
- B.** The policies are updated annually.
- C.** Senior management supports the policies.
- D.** The policies are aligned to industry best practices.

Answer: ([SHOW ANSWER](#))

The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization's leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization's goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.

Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing information security policies. The policies should be relevant and applicable to the employees' roles and functions, and should be reinforced by regular training and awareness programs.

The policies should be updated periodically to reflect the changes in the organization's environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.

The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization's specific context, needs, and

expectations, and should be consistent with the organization's vision, mission, and values.

References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1009.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 242

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. Features of data protection products
- C. Data classification policy
- D. Data storage procedures

Answer: (SHOW ANSWER)

NEW QUESTION: 243

Which of the following MOST effectively identifies the organization's ability to comply with legal, regulatory, and contractual requirements?

- A. Vulnerability scan
- B. Control self-assessment (CSA)
- C. Gap analysis
- D. Risk assessment

Answer: (SHOW ANSWER)

A gap analysis is the most effective method to identify an organization's ability to comply with legal, regulatory, and contractual requirements because it explicitly compares the current state of controls, policies, and practices against required obligations. In CISM governance, compliance is assessed by determining whether mandatory requirements are fully met, partially met, or not met at all-this is the precise purpose of a gap analysis.

Vulnerability scanning (A) focuses on technical weaknesses and does not assess compliance with laws or contracts. A control self-assessment (CSA) (B) evaluates the effectiveness of existing controls but does not systematically compare them against external compliance requirements. A risk assessment (D) evaluates threats, vulnerabilities, and impacts, but its objective is risk prioritization, not compliance determination.

CISM emphasizes that governance requires clear visibility into compliance gaps so management can prioritize remediation, allocate resources, and demonstrate due diligence. Gap analysis provides structured, auditable evidence of compliance posture and directly supports regulatory readiness and contractual assurance.

References:

ISACA CISM Review Manual, Information Security Governance - compliance management and gap analysis ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 244

A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

- A. The time and location that the breach occurred
- B. Evidence of previous incidents caused by the user
- C. The underlying reason for the user error
- D. Appropriate disciplinary procedures for user error

Answer: ([SHOW ANSWER](#))

The underlying reason for the user error is the most important factor to determine during the post-incident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents. References = CISM Review Manual 2023, page

1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

NEW QUESTION: 245

To optimize the implementation of information security governance in an organization, an information security manager should:

- A. Make gradual changes to governance to minimize employee resistance
- B. Ensure change control processes are in place
- C. Utilize existing governance structures when possible
- D. Implement processes consistent with international standards

Answer: ([SHOW ANSWER](#))

The correct answer is C because information security governance is most effectively implemented when it is integrated into existing enterprise governance structures wherever possible. Using established committees, reporting channels, risk management processes, decision-making bodies, and accountability mechanisms improves adoption and avoids creating isolated or duplicative security governance processes. It also helps ensure that information security is treated as part of enterprise governance rather than as a separate technical function. Gradual change may reduce resistance in some situations, but it is not the best general approach to optimizing governance implementation. Change control processes are useful for managing system or process changes, but they do not optimize the overall governance structure. International standards can provide useful guidance, but implementing standard-based processes without considering the organization's existing governance model may reduce effectiveness. CISM governance principles emphasize alignment with business objectives, integration with enterprise governance, senior management oversight, and clear accountability. Therefore, utilizing existing governance structures is the best way to optimize implementation. Reference: CISM Information Security Governance; enterprise governance integration, governance structures, accountability, and strategic alignment principles.

NEW QUESTION: 246

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 in 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: 247

Which of the following would BEST ensure that security is integrated during application development?

- A.** Employing global security standards during development processes

- B. Providing training on secure development practices to programmers
- C. Performing application security testing during acceptance testing
- D. Introducing security requirements during the initiation phase

Answer: ([SHOW ANSWER](#))

Introducing security requirements during the initiation phase would BEST ensure that security is integrated during application development because it would allow the security objectives and controls to be defined and aligned with the business needs and risk appetite before any design or coding is done. This would also facilitate the security by design approach, which is the most effective method to enhance the security of applications and application development activities¹. Introducing security requirements early would also enable the collaboration between security professionals and developers, the identification and specification of security architectures, and the integration and testing of security controls throughout the development life cycle². Employing global security standards during development processes (A) would help to ensure the consistency and quality of security practices, but it would not necessarily ensure that security is integrated during application development. Providing training on secure development practices to programmers (B) would help to raise the awareness and skills of developers, but it would not ensure that security is integrated during application development. Performing application security testing during acceptance testing would help to verify the security of the application before deployment, but it would not ensure that security is integrated during application development. It would also be too late to identify and remediate any security issues that could have been prevented or mitigated earlier in the development process. References = 1: Five Key Components of an Application Security Program - ISACA¹; 2: CISM Domain - Information Security Program Development | Infosec²

NEW QUESTION: 248

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: 249

Which of the following should be done FIRST after a ransomware incident has been successfully contained?

- A. Restore impacted systems.
- B. Conduct forensic analysis.
- C. Notify relevant stakeholders.
- D. Perform lessons learned.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 250

A business impact analysis (BIA) BEST enables an organization to establish:

- A. restoration priorities.
- B. recovery methods.
- C. annualized loss expectancy (ALE).
- D. total cost of ownership (TCO).

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 251

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: 252

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

- 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: 253

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

NEW QUESTION: 254

Of the following, who is BEST suited to own the risk discovered in an application?

- A. Information security manager
- B. Senior management
- C. Control owner
- D. System owner

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 255

Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

- A. Isolate affected systems to prevent the spread of damage
- B. Determine the final root cause of the incident
- C. Mitigate exploited vulnerabilities to prevent future incidents
- D. Remove all instances of the incident from the network

Answer: ([SHOW ANSWER](#))

The containment phase focuses on limiting the scope of the incident. Isolating affected systems immediately helps prevent propagation and further compromise.

"During the containment phase, isolating compromised systems is a key tactic to minimize further impact and enable safe recovery."

- CISM Review Manual 15th Edition, Chapter 4: Incident Response Life Cycle, Section: Containment Strategies*

NEW QUESTION: 256

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>

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam

questions have been updated and answers have been corrected get the **newest** EduDump.com CISM dumps with Test Engine here:
<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 257

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

NEW QUESTION: 258

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: 259

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: 260

Which of the following provides the BEST assurance that security policies are applied across business operations?

- A. Organizational standards are included in awareness training.
- B. Organizational standards are enforced by technical controls.
- C. Organizational standards are required to be formally accepted.
- D. Organizational standards are documented in operational procedures.

Answer: ([SHOW ANSWER](#))

= The best assurance that security policies are applied across business operations is that organizational standards are documented in operational procedures. Operational procedures are the specific steps and actions that need to be taken to implement and comply with the security policies and standards. They provide clear and consistent guidance for the staff members who are responsible for performing the security tasks and functions. They also help to ensure that the security policies and standards are aligned with the business objectives and processes, and that they are measurable and auditable. Documenting the organizational standards in operational procedures can help to improve the security awareness, accountability, and performance of the staff members, and to reduce the risks of errors, deviations, and violations. The other options are not the best assurance because they are either too general or too specific. Organizational standards are included in awareness training (A) is a good practice to educate the staff members about the security policies and standards, but it does not guarantee that they will follow them or understand how to apply them in their daily operations. Organizational standards are enforced by technical controls (B) is a way to automate and monitor the compliance with the security policies and standards, but it does not cover all the aspects of security that may require human intervention or judgment. Organizational standards are required to be formally accepted is a way to obtain the commitment and support from the staff members for the security policies and standards, but it does not ensure that they will adhere to them or know how to execute them in their work activities. References = CISM Review Manual 2022, pages 24-25, 28-29; CISM Item Development Guide 2022, page 9; Policies, Procedures, Standards, Baselines, and Guidelines | CISSP Security- Management Practices | Pearson IT Certification

NEW QUESTION: 261

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

- 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: B ([LEAVE A REPLY](#))

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: 262

Reverse lookups can be used to prevent successful:

- A. denial of service (DoS) attacks
- B. session hacking
- C. phishing attacks
- D. Internet protocol (IP) spoofing

Answer: (SHOW ANSWER)

Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

NEW QUESTION: 263

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: 264

Which of the following is the BEST way to monitor the effectiveness of security controls?

- A. Benchmark security controls against similar organizations
- B. Review application and system audit logs
- C. Establish and report security metrics
- D. Conduct regular threat assessments

Answer: ([SHOW ANSWER](#))

The correct answer is C because security metrics provide measurable evidence of whether controls are operating effectively and achieving intended outcomes. Establishing and reporting metrics allows the information security manager to monitor trends, identify control weaknesses, support management decisions, and demonstrate program performance. Benchmarking can provide useful external comparison, but it does not directly measure the organization's own control effectiveness. Reviewing audit logs is valuable for specific detective controls, but it is too narrow to monitor the overall effectiveness of security controls. Threat assessments help identify changing threat conditions, but they do not directly show whether controls are performing as intended. CISM emphasizes performance measurement, monitoring, and reporting as essential components of managing an information security program. Metrics should be aligned with security objectives, risk appetite, and business goals. Effective metrics allow management to determine whether controls remain appropriate, efficient, and effective in reducing risk to acceptable levels. Reference: CISM Information Security Program Development and Management; security metrics, control monitoring, and performance reporting principles.

NEW QUESTION: 265

Which of the following is the MOST effective way to ensure information security policies are understood?

- A. Implement a whistle-blower program.
- B. Provide regular security awareness training.

- C. Include security responsibilities in job descriptions.
- D. Document security procedures.

Answer: ([SHOW ANSWER](#))

Security awareness training is the most effective way to ensure information security policies are understood, as it educates employees on the purpose, content and importance of the policies, and how to comply with them. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

NEW QUESTION: 266

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: 267

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: 268

Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?

- A.** Review the previous risk assessment and countermeasures.
- B.** Perform a new risk assessment,
- C.** Evaluate countermeasures to mitigate new risks.
- D.** Transfer the new risk to a third party.

Answer: (SHOW ANSWER)

According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A risk assessment helps to determine the current level of risk exposure and the adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.

The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options.

References = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

NEW QUESTION: 269

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: 270

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

- A. Information technology
- B. Information security
- C. Human resources (HR)
- D. Legal

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 271

Which of the following is MOST important to consider when determining asset valuation?

- A. Asset recovery cost
- B. Asset classification level
- C. Cost of insurance premiums
- D. Potential business loss

Answer: ([SHOW ANSWER](#))

Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important as potential business loss, as they do not capture the full value

of the asset to the organization. References = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

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

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 272

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 the incident to occur. Identifying the root cause helps to prevent or mitigate future incidents, as well as to improve the incident response process. Re-evaluating the impact of incidents, identifying vulnerabilities, and identifying control improvements are secondary objectives of a post-incident review, which are derived from the root cause analysis. References = CISM Review Manual, 16th Edition, page 3061; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1512 The primary objective of performing a post-incident review is to identify the root cause of the incident. After an incident has occurred, the post-incident review process involves gathering and analyzing evidence to determine the cause of the incident. This analysis will help to identify both the underlying vulnerability that allowed the incident to occur, as well as any control improvements that should be implemented to prevent similar incidents from occurring in the future. Additionally, the post-incident review process can also be used to re-evaluate the impact of the incident, as well as any potential implications for the organization.

NEW QUESTION: 273

Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?

- A. Ensure security is involved in the procurement process.
- B. Conduct an information security audit on the third-party vendor.
- C. Communicate security policy with the third-party vendor.
- D. Review the third-party contract with the organization's legal department.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 274

Which of the following components of an information security risk assessment is MOST valuable to senior management?

- A. Threat profile
- B. Residual risk
- C. Return on investment (ROI)
- D. Mitigation actions

Answer: ([SHOW ANSWER](#))

Residual risk is the risk that remains after implementing risk mitigation actions. It is the most valuable component for senior management because it helps them to evaluate the effectiveness and efficiency of risk management and make informed decisions about risk acceptance, transfer or avoidance. References = CISM Review Manual, 16th Edition, Chapter 2, Section 2.3.41

NEW QUESTION: 275

Which of the following is the BEST approach to make strategic information security decisions?

- A. Establish regular information security status reporting.
- B. Establish an information security steering committee.
- C. Establish business unit security working groups.
- D. Establish periodic senior management meetings.

Answer: ([SHOW ANSWER](#))

= According to the CISM Review Manual (Digital Version), page 9, an information security steering committee is a group of senior managers from different business units and functions who provide guidance and oversight for the information security program. An information security steering committee is the best approach to make strategic information security decisions because it can:

Ensure alignment of information security strategy with business objectives and risk appetite¹
Facilitate communication and collaboration among different stakeholders and promote information security awareness and culture²
Provide direction and support for information security initiatives and projects³
Monitor and review the performance and effectiveness of the information security program⁴
Resolve conflicts and issues related to information security policies and practices⁵
Establishing regular information security status reporting, business unit security working groups, and periodic senior management meetings are useful activities for information security management, but they are not sufficient to make strategic information security decisions without the involvement and guidance of an information security steering committee. References = 1: CISM Review Manual (Digital Version), page

9 2: 1 3: 2 4: 3 5: 4

An Information Security Steering Committee is a group of stakeholders responsible for providing governance and guidance to the organization on all matters related to information security. The committee provides oversight and guidance on security policies, strategies, and technology

implementation. It also ensures that the organization is in compliance with relevant laws and regulations. Additionally, it serves as a forum for discussing security-related issues and ensures that security is taken into account when making strategic decisions.

NEW QUESTION: 276

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: 277

Which of the following is MOST important to include in monthly information security reports to the board?

- A.** Trend analysis of security metrics
- B.** Risk assessment results
- C.** Root cause analysis of security incidents
- D.** Threat intelligence

Answer: ([SHOW ANSWER](#))

The most important information to include in monthly information security reports to the board is the trend analysis of security metrics. Security metrics are quantitative and qualitative measures that indicate the performance and effectiveness of the information security program and the alignment with the business objectives. Trend analysis is the process of comparing and evaluating the changes and patterns of security metrics over time. Trend analysis can help to identify the strengths and weaknesses of the information security program, the progress and achievements of the security goals and initiatives, the gaps and opportunities for improvement,

and the impact and value of the information security investments. Trend analysis can also help to communicate the current and future security risks and challenges, and the recommended actions and strategies to address them. Trend analysis can provide the board with a clear and concise overview of the information security status and direction, and enable informed and timely decision making.

References =

- * CISM Review Manual 15th Edition, page 1631
- * The CISO's Guide to Reporting Cybersecurity to the Board2
- * CISM 2020: Information Security Metrics and Reporting, video 13

NEW QUESTION: 278

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: (SHOW ANSWER)

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: 279

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: 280

The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

- A. enhance the organization's antivirus controls.
- B. eliminate the risk of data loss.
- C. complement the organization's detective controls.
- D. reduce the need for a security awareness program.

Answer: ([SHOW ANSWER](#))

A data loss prevention (DLP) solution is a type of detective control that monitors and prevents unauthorized transmission or leakage of sensitive data from the organization. A DLP solution can enhance the organization's antivirus controls by detecting and blocking malicious code that attempts to exfiltrate data, but this is not its main benefit. A DLP solution cannot eliminate the risk of data loss, as there may be other sources of data loss that are not covered by the DLP solution, such as physical theft, accidental deletion, or natural disasters. A DLP solution also does not reduce the need for a security awareness program, as human factors are often the root cause of data loss incidents. A security awareness program can educate and motivate employees to follow security policies and best practices, and to report any suspicious or anomalous activities.

References = ISACA, CISM Review Manual, 16th Edition, 2020, page 79.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1003.

NEW QUESTION: 281

Which of the following is the MOST effective way to detect security incidents?

- A. Analyze recent security risk assessments.
- B. Analyze security anomalies.
- C. Analyze penetration test results.
- D. Analyze vulnerability assessments.

Answer: ([SHOW ANSWER](#))

Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

NEW QUESTION: 282

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: 283

A newly appointed information security manager of a retailer with multiple stores discovers an HVAC (heating, ventilation, and air conditioning) vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. Which of the following should be the information security manager's FIRST course of action?

- A. Conduct a penetration test of the vendor.
- B. Review the vendor's technical security controls
- C. Review the vendor contract
- D. Disconnect the real-time access

Answer: (SHOW ANSWER)

Reviewing the vendor contract should be the information security manager's first course of action when discovering an HVAC vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. The vendor contract should specify the terms and conditions of the vendor's access to the retailer's network, such as the scope, purpose, duration, frequency, and method of access. The vendor contract should also define the roles and responsibilities of both parties regarding security, privacy, compliance, liability, and incident response. Reviewing the vendor contract will help the information security manager to understand the contractual obligations and expectations of both parties, and to identify any gaps or issues that need to be addressed or resolved¹. The other options are not the first course of action for the information security manager when discovering an HVAC vendor has remote access to the stores. Conducting a penetration test of the vendor may be a useful way to assess the vendor's security posture and potential vulnerabilities, but it should be done with the vendor's consent and cooperation, and after reviewing the vendor contract².

Reviewing the vendor's technical security controls may be a necessary step to verify the vendor's compliance with security standards and best practices, but it should be done after reviewing the vendor contract and in accordance with the agreed-upon audit procedures³. Disconnecting the real-time access may be a drastic measure that could disrupt the vendor's service delivery and violate the vendor contract, unless there is a clear and imminent threat or breach that warrants such action. References: 1: Vendor Access: Addressing the Security Challenge with Urgency - BeyondTrust 2: Penetration Testing - NIST 3: Reduce Risk from Third Party Access | BeyondTrust : Third-Party Vendor Security Risk Management & Prevention

NEW QUESTION: 284

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: ([SHOW ANSWER](#))

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: 285

When remote access is granted to a company's internal network, the MOST important consideration should be that access is provided:

- A. subject to legal and regulatory requirements.
- B. if a robust IT infrastructure exists.
- C. on a need-to-know basis subject to controls.
- D. by the use of a remote access server.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 286

Which of the following is the MOST significant contributor to the success of incident response efforts during a major breach?

- A. The incident response plan is aligned with the disaster recovery strategy
- B. The incident response process is regularly tested
- C. Incident response processes are documented and available to staff
- D. The incident response plan clearly outlines roles and responsibilities

Answer: ([SHOW ANSWER](#))

Clear roles and responsibilities (D) are the most significant contributor to effective incident response during a major breach. CISM emphasizes that confusion over authority, decision-making, or responsibilities severely hinders response effectiveness. While testing (B), documentation (C), and alignment with DR (A) are important, clearly defined roles ensure rapid, coordinated action under pressure.

References: ISACA CISM Review Manual (Incident management-roles, responsibilities, and coordination); CISM Exam Content Outline (Domain 4).

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 287

Which of the following is MOST important to determine following the discovery and eradication of a malware attack?

- A. The malware entry path
- B. The type of malware involved
- C. The method of detecting the malware
- D. The creator of the malware

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 288

An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

- A. Internal IT audit
- B. The data custodian
- C. The information security manager
- D. The data owner

Answer: (SHOW ANSWER)

The data owner is the person who has the authority and responsibility to classify, grant access, and monitor the use of the CRM data. The data owner should ensure that the data is protected according to its classification and business requirements. The data custodian is the person who implements the controls and procedures to protect the data as directed by the data owner. The information security manager is the person who advises the data owner on the best practices and standards for data security. The internal IT audit is the function that evaluates the effectiveness and compliance of the data security controls and procedures.

References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Roles and Responsibilities, Subsection: Data Owner, Page 23.

NEW QUESTION: 289

A recent application security assessment identified a number of low- and medium-level vulnerabilities. Which of the following stakeholders is responsible for deciding the appropriate risk treatment option?

- A. Security manager
- B. Chief information security officer (CISO)
- C. System administrator
- D. Business owner

Answer: (SHOW ANSWER)

Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3, "The appropriate risk treatment option is decided by the chief information security officer (CISO) or the designated risk owner."¹ The CISO is the senior executive who is responsible for overseeing and managing the information security program of an organization. The CISO has the authority and expertise to assess the risks, determine the risk appetite and tolerance levels, and select the most suitable risk treatment options for each risk. The CISO also has the accountability and responsibility for implementing, monitoring, and reporting on the risk treatment activities.

References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3

NEW QUESTION: 290

Which of the following is the GREATEST challenge with assessing emerging risk in an organization?

- A. Lack of a risk framework
- B. Ineffective security controls
- C. Presence of known vulnerabilities
- D. Incomplete identification of threats

Answer: (SHOW ANSWER)

The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed. Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The

other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment.

References:

* <https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.html>

* <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging-risk-analysis>

* <https://projectriskcoach.com/emerging-risks/>

NEW QUESTION: 291

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. Immediately suspend the executives' access privileges.
- C. Notify the CISO of the security policy violation.
- D. Perform a system access review.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 292

A hacking group has posted an organization's employee data on social media. What should the information security manager do FIRST?

- A. Inform the impacted employees.
- B. Initiate the incident response process.
- C. Escalate to senior management.
- D. Engage a forensic analysis team.

Answer: ([SHOW ANSWER](#))

The first action the information security manager should take is to initiate the incident response process (B).

According to CISM incident management principles, once there is confirmed evidence of a security incident- such as employee data being publicly disclosed-the organization must immediately activate its formal incident response procedures. This ensures that actions are coordinated, evidence is preserved, roles and responsibilities are clear, and regulatory, legal, and communication requirements are handled in a controlled manner.

Informing impacted employees (A), escalating to senior management (C), and engaging forensic experts (D) are all important steps, but they are subsequent actions that occur within the incident response process, not before it. Initiating the incident response process provides the structured framework needed to assess scope, contain damage, meet notification obligations, and determine whether forensic investigation is required.

CISM emphasizes that ad hoc actions taken outside the incident response process increase the risk of miscommunication, legal exposure, and ineffective containment. Activating the process first ensures disciplined execution aligned with governance, legal, and regulatory expectations.

References:

ISACA CISM Review Manual, Information Security Incident Management - incident response lifecycle and escalation ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 293

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

- A. Set up communication channels for the target audience.
- B. Determine the needs and requirements of each audience.
- C. Create a comprehensive singular communication
- D. Invoke the organization's incident response plan.

Answer: ([SHOW ANSWER](#))

The information security manager should do FIRST invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a comprehensive singular communication are all important steps for communicating effectively with the board, regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the relevant information to the target audience according to the plan. References = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012

Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

NEW QUESTION: 294

Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

- A. Legal and regulatory requirements
- B. Likelihood of a disaster
- C. Organizational tolerance to service interruption
- D. Geographical location of the backup site

Answer: (SHOW ANSWER)

= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. References = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 792 Learn more:

1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 295

Prior to conducting a forensic examination, an information security manager should:

- A. boot the original hard disk on a clean system.
- B. create an image of the original data on new media.
- C. duplicate data from the backup media.
- D. shut down and relocate the server.

Answer: (SHOW ANSWER)

= A forensic examination is a process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable. The first step in conducting a forensic examination is to create an image of the original data on new media, such as a hard disk, a CD-ROM, or a USB drive. This is done to ensure that the original data is not altered, damaged, or destroyed during the examination. An image is an exact copy of the data, including the file system, the slack space, and the deleted files. Creating an image also allows the examiner to work on a duplicate of the data, rather than the original, which may be needed as evidence in court. Booting the original hard disk on a clean system is not a good practice, as it may change the data on the disk, such as the timestamps, the registry entries, and the log files. Duplicating data from the backup media is not sufficient, as the backup media may not contain all the data that is relevant to the investigation, such as the deleted files, the temporary files, and the swap files. Shutting down and relocating the server is not advisable, as it may cause data loss, corruption, or tampering. The server should be kept running and isolated from the network until an image is created. References = CISM Review Manual 15th Edition, page 204-205.

Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

NEW QUESTION: 296

A penetration test was conducted by an accredited third party. Which of the following should be the information security manager's FIRST course of action?

- A. Ensure vulnerabilities found are resolved within acceptable timeframes
- B. Ensure a risk assessment is performed to evaluate the findings
- C. Request funding needed to resolve the top vulnerabilities
- D. Report findings to senior management

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 297

Which of the following is a PRIMARY reason for senior management to review reports on information security?

- A. To assess the effectiveness of the security program
- B. To ensure adequate security resources are available
- C. To confirm security audits are regularly performed
- D. To ensure security risk is managed cost-effectively

Answer: ([SHOW ANSWER](#))

The correct answer is A because senior management reviews information security reports to determine whether the security program is achieving its objectives and effectively supporting the organization's business goals. Reporting provides visibility into program performance, risk trends, incident activity, compliance status, control effectiveness, and progress against security objectives. Ensuring adequate resources is an important management responsibility, but resource decisions should be based on an understanding of program effectiveness and risk. Confirming regular audits is useful, but audits are only one source of assurance.

Ensuring risk is managed cost-effectively is also important, but it is a broader outcome of governance and decision-making. The primary purpose of reporting is to give senior management enough information to evaluate whether the program is performing as intended. In CISM governance, reporting enables oversight, accountability, informed decision-making, and alignment between security and enterprise objectives.

Therefore, assessing the effectiveness of the security program is the best answer.

Reference: CISM Information Security Governance; management reporting, program effectiveness, governance oversight, and performance measurement principles.

NEW QUESTION: 298

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: 299

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

- 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: 300

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

- A. best practices.
- B. control framework
- C. regulatory requirements.
- D. cost-benefit analysis,

Answer: (SHOW ANSWER)

Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls¹².

CBA involves the following steps¹²:

Identify the objectives and scope of the analysis

Identify the alternatives and options for achieving the objectives

Identify and quantify the costs and benefits of each alternative

Compare the costs and benefits of each alternative using a common metric or criteria
Select the alternative that maximizes the net benefit or minimizes the net cost
Perform a sensitivity analysis to test the robustness and validity of the results
Document and communicate the results and recommendations
CBA is mainly driven by the information security manager's decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization. Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization's objectives, resources, and environment¹².
References = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

NEW QUESTION: 301

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. Review the cloud provider's service level agreement (SLA).
- B. Identify users associated with the exposed data.
- C. Invoke the incident response plan.
- D. Initiate the organization's data loss prevention (DLP) processes.

Answer: ([SHOW ANSWER](#))

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 302

A global organization is developing an incident response team. The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events. Which of the following BEST supports these objectives?

- A. Virtual incident response team
- B. Distributed incident response team
- C. Outsourced incident response team
- D. Centralized incident response team

Answer: ([SHOW ANSWER](#))

A centralized incident response team ensures consistent communication, coordination, and a unified approach to managing incidents across the organization.

"A centralized incident response team provides a consistent and coordinated approach to incident handling and ensures that management is kept informed."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Organization Models*

NEW QUESTION: 303

Which of the following is the MOST important requirement for a successful security program?

- A. Mapping security processes to baseline security standards
- B. Penetration testing on key systems
- C. Management decision on asset value
- D. Nondisclosure agreements (NDA) with employees

Answer: ([SHOW ANSWER](#))

"A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value."

NEW QUESTION: 304

When properly implemented, secure transmission protocols protect transactions:

- A.** from eavesdropping.
- B.** from denial of service (DoS) attacks.
- C.** on the client desktop.
- D.** in the server's database.

Answer: ([SHOW ANSWER](#))

Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information¹. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party.

Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage². Therefore, secure transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures³. Some examples of secure transmission protocols are:

- * Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.

- * Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses

two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.

* Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port forwarding, which allows secure tunneling of other network services through SSH connections.

References = 1: 6 Network Security Protocols You Should Know | Cato Networks 2:

Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL

/TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec - Wikipedia : Secure Shell - Wikipedia

NEW QUESTION: 305

Which of the following BEST protects against emerging advanced persistent threat (APT) actors?

- A. Honeypot environment
- B. Updated security awareness materials
- C. Ongoing incident response training
- D. Proactive monitoring

Answer: (SHOW ANSWER)

Proactive monitoring (e.g., threat hunting, real-time log analysis, anomaly detection) is the most effective defense against Advanced Persistent Threats (APTs), which are stealthy, well-resourced, and long-term attacks.

APT actors:

Use zero-day exploits

Maintain long-term unauthorized access

Avoid detection

Traditional controls often fail. Proactive monitoring detects anomalies early, allowing for faster mitigation.

"Ongoing monitoring and detection programs are essential for identifying and responding to persistent and evolving threats."

- CISM Review Manual 15th Edition, Chapter 4: Threat Management, Section: APT Detection Techniques*

NEW QUESTION: 306

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: (SHOW ANSWER)

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: 307

Which of the following would provide the BEST evidence to senior management that security control performance has improved?

- A. Demonstrated return on security investment
- B. Reduction in inherent risk
- C. Results of an emerging threat analysis
- D. Review of security metrics trends

Answer: D (LEAVE A REPLY)

Review of security metrics trends is the best evidence to senior management that security control performance has improved because it helps to measure and demonstrate the effectiveness and efficiency of the security controls over time. Security metrics are quantitative or qualitative indicators that provide information about the security status or performance of an organization, system, process, or activity. Security metrics can be used to evaluate the implementation, operation, and outcome of security controls, such as the number of vulnerabilities detected and remediated, the time to respond and recover from incidents, the compliance level with security policies and standards, or the return on security investment. Review of security metrics trends helps to identify and communicate the progress, achievements, and challenges of the security program, as well as to support decision making and continuous improvement. Therefore, review of security metrics trends is the correct answer.

References:

<https://www.bitsight.com/blog/importance-continuous-improvement-security-performance-management>

<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2>

<https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary-cybersecurity-performance-goals>.

NEW QUESTION: 308

Which of the following is the MOST important consideration when briefing executives about the current state of the information security program?

- A. Including a situational forecast
- B. Using appropriate language for the target audience
- C. Including trend charts for metrics

D. Using a rating system to demonstrate program effectiveness

Answer: ([SHOW ANSWER](#))

= When briefing executives about the current state of the information security program, the most important consideration is to use appropriate language for the target audience. This means avoiding technical jargon, acronyms, and details that may confuse or bore the executives, and instead focusing on the business value, risks, and benefits of the information security program. The other options are not as important or relevant as using appropriate language, although they may also be useful to include in the briefing. For example, a situational forecast may be helpful to show the future trends and challenges, but it is not as essential as communicating the current state clearly and concisely. Similarly, trend charts for metrics and a rating system to demonstrate program effectiveness may be useful to support the briefing, but they are not as critical as using language that the executives can understand and relate to. References = Information Security Guide for Government Executives, page 7: "Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment." Information security guide for government executives - NIST, page 3: "The executive should communicate the importance of information security to the organization and its staff, using language that is meaningful to the target audience." Information Security Committee Charter - SecurityStudio, page 1: "The committee also coordinates and communicates the direction, current state, and oversight of the information security program."

NEW QUESTION: 309

When performing a business impact analysis (BIA), who should be responsible for determining the initial recovery time objective (RTO)?

- A. External consultant**
- B. Information owners**
- C. Information security manager**
- D. Business continuity coordinator**

Answer: ([SHOW ANSWER](#))

Information owners are responsible for determining the initial recovery time objective (RTO) for their information assets and processes, as they are the ones who understand the business requirements and impact of a disruption. An external consultant may assist in conducting the business impact analysis (BIA), but does not have the authority to decide the RTO. An information security manager may provide input on the security aspects of the RTO, but does not have the business perspective to determine the RTO. A business continuity coordinator may facilitate the BIA process and ensure the alignment of the RTO with the business continuity plan, but does not have the ownership of the information assets and processes. References = CISM Review Manual 15th Edition, page 202.

When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the BIA and should be determined in cooperation with the information owners. The

RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

NEW QUESTION: 310

An information security team must obtain approval from the information security steering committee to implement a key control. Which of the following is the MOST important input to assist the committee in making this decision?

- A. Risk assessment
- B. Security architecture
- C. IT strategy
- D. Business case

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 311

A Seat a-hosting organization's data center houses servers, appli
BEST approach for developing a physical access control policy for the organization?

- A. Review customers' security policies.
- B. Conduct a risk assessment to determine security risks and mitigating controls.
- C. Develop access control requirements for each system and application.
- D. Design single sign-on (SSO) or federated access.

Answer: ([SHOW ANSWER](#))

= The best approach for developing a physical access control policy for the organization is to conduct a risk assessment to determine the security risks and mitigating controls that are relevant and appropriate for the organization's data center. A risk assessment is a process of identifying, analyzing, and evaluating the information security risks that could affect the availability, integrity, or confidentiality of the servers, applications, and data that are hosted in the data center. A risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate physical access to the data center, such as theft, damage, sabotage, or espionage, and the potential consequences for the organization and its customers, such as service disruption, data loss, data breach, or legal liability. A risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to prevent, detect, or respond to the physical access incidents, such as locks, alarms, cameras, guards, badges, or logs. A risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the physical access control policy and the risk management process.

Reviewing customers' security policies, developing access control requirements for each system and application, and designing single sign-on (SSO) or federated access are all possible steps that the organization can take after conducting the risk assessment, but they are not the best ones. Reviewing customers' security policies is a process of understanding and complying with the customers' expectations and requirements for the security of their servers, applications, and

data that are hosted in the data center, and ensuring that the organization's physical access control policy is consistent and compatible with them. Developing access control requirements for each system and application is a process of defining and implementing the specific rules and criteria for granting or denying the physical access to the servers and applications that are hosted in the data center, based on the roles, responsibilities, and privileges of the users, and the sensitivity and criticality of the systems and applications. Designing single sign-on (SSO) or federated access is a process of enabling and facilitating the authentication and authorization of the users who need to access the servers and applications that are hosted in the data center, by using a single or shared identity and credential across multiple systems and domains. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1542

NEW QUESTION: 312

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/>

NEW QUESTION: 313

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: 314

Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?

- A. Parallel test
- B. Full interruption test
- C. Simulation test
- D. Tabletop test

Answer: (SHOW ANSWER)

A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required. A parallel test involves processing the same transactions or data at both the primary and the alternate site simultaneously, and comparing the results for accuracy and consistency. A parallel test can validate the functionality, performance, and reliability of the alternate site without disrupting the normal operations at the primary site. A parallel test can also identify and resolve any issues or discrepancies between the two sites before a real disaster occurs. A parallel test can provide a high level of assurance and confidence that the alternate site can support the organization's continuity requirements.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP) Testing, page 1861; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 56, page 522.

A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required because it involves processing data at both the primary and alternate sites simultaneously without disrupting the normal operations¹. A full interruption test would cause downtime and potential loss of data or revenue². A simulation test would not provide a realistic assessment of the alternate site's capabilities³. A tabletop test would only involve a discussion of the procedures and scenarios without actually testing the site⁴.

1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM - ISACA Certified Information Security Manager Exam Prep - NICCS 3: Prepare for the ISACA Certified Information Security Manager Exam: CISM ... 4: CISM: Certified Information Systems Manager | Official ISACA ... - NICCS

NEW QUESTION: 315

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: 316

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]

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 317

Which of the following is the BEST indication that an organization has integrated information security governance with corporate governance?

- A. Security performance metrics are measured against business objectives.
- B. Impact is measured according to business loss when assessing IT risk.
- C. Security policies are reviewed whenever business objectives are changed.
- D. Service levels for security vendors are defined according to business needs.

Answer: (SHOW ANSWER)

Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives.

Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 318

Which of the following events is MOST likely to require an organization to revisit its information security framework?

- A. New services offered by IT
- B. Changes to the risk landscape

- C. A recent cybersecurity attack
- D. A new technology implemented

Answer: B ([LEAVE A REPLY](#))

Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

NEW QUESTION: 319

A security review identifies that confidential information on the file server has been accessed by unauthorized users in the organization. Which of the following should the information security manager do FIRST?

- A. Invoke the incident response plan
- B. Implement role-based access control (RBAC)
- C. Remove access to the information
- D. Delete the information from the file server

Answer: ([SHOW ANSWER](#)**)**

The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.

"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution* ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

NEW QUESTION: 320

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: 321

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: 322

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: 323

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

- A. List of recent security events
- B. Key risk indication (KRIs)
- C. Review of information security policies
- D. information security budget requests

Answer: (SHOW ANSWER)

Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References:

<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004>

NEW QUESTION: 324

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: 325

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.

NEW QUESTION: 326

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: 327

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?

- A. Ensuring hashing of administrator credentials
- B. Enforcing service level agreements (SLAs)
- C. Ensuring encryption for data in transit
- D. Utilizing a formal change management process

Answer: (SHOW ANSWER)

Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

NEW QUESTION: 328

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: (SHOW ANSWER)

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: 329

Which of the following is MOST effective for communicating forward-looking trends within security reporting?

- A.** Key control indicator (KCI)
- 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: 330

Which of the following provides the MOST useful information for identifying security control gaps on an application server?

- A. Risk assessments
- B. Threat models
- C. Penetration testing
- D. Internal audit reports

Answer: (SHOW ANSWER)

Penetration testing is the most useful method for identifying security control gaps on an application server because it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application server. Penetration testing can reveal the actual impact and risk of the security control gaps, and provide recommendations for remediation and improvement.

References: The CISM Review Manual 2023 defines penetration testing as "a method of evaluating the security of an information system or network by simulating an attack from a malicious source" and states that

"penetration testing can help identify security control gaps and provide evidence of the potential impact and risk of the gaps" (p. 185). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Penetration testing is the correct answer because it is the most useful method for identifying security control gaps on an application server, as it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application server, and provides recommendations for remediation and improvement" (p. 95). Additionally, the web search result 4 states that "penetration testing is a valuable tool for discovering security gaps in your application server and network infrastructure" and that

"penetration testing can help you assess the effectiveness and efficiency of your security controls, and identify the areas that need improvement or enhancement" (p. 1).

NEW QUESTION: 331

Which of the following should have the MOST influence on the development of information security policies?

- A. Business strategy
- B. Past and current threats
- C. IT security framework
- D. Industry standards

Answer: (SHOW ANSWER)

Business strategy is the overarching driver for any organizational initiative, including security. Information security policies must align with the strategic goals of the organization to ensure relevance, support, and effectiveness.

Security policies that do not consider the business context may hinder operations or fail to protect key objectives. Business-driven policies are more likely to gain executive support and compliance from stakeholders, creating a strong foundation for governance.

"Information security policies must be aligned with business goals and objectives to ensure that they support the overall mission and are embraced by stakeholders."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Strategy Alignment*

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 332

Which of the following is the BEST way to obtain organization-wide support for an information security program?

- A. Mandate regular security awareness training.
- B. Develop security performance metrics.
- C. Position security as a business enabler.
- D. Prioritize security initiatives based on IT strategy.

Answer: (SHOW ANSWER)

Positioning security as a business enabler is the BEST way to obtain organization-wide support for an information security program, because it helps to demonstrate the value and benefits of security to the organization's strategic objectives, performance, and reputation. By aligning security with the business goals and needs, the information security manager can gain the buy-in and commitment of senior management and other stakeholders, and foster a positive security culture across the organization.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "The information security manager should position information security as a business enabler that supports the achievement of the enterprise's business objectives and adds value to the enterprise." CISM Review Manual, 16th Edition, ISACA, 2020, p. 39: "The information security manager should communicate the value and benefits of information security to senior management and other stakeholders to obtain their support and commitment for the information security program." CISM Review Manual, 16th Edition, ISACA, 2020, p. 40: "The information security manager should promote a positive security culture within the enterprise by influencing the behavior and attitude of employees and other parties toward information security."

NEW QUESTION: 333

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: 334

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 in 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: 335

An organization is about to purchase a rival organization. The PRIMARY reason for performing information security due diligence prior to making the purchase is to:

- A. determine the security exposures.
- B. assess the ability to integrate the security department operations.
- C. ensure compliance with international standards.
- D. evaluate the security policy and standards.

Answer: A ([LEAVE A REPLY](#))

Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value, reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.

References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnaire

NEW QUESTION: 336

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: 337

Which of the following BEST enables users to recover from ransomware or malware attacks?

- A. Incident response plans
- B. Frequent system backups
- C. Regular antivirus updates
- D. End-user awareness training

Answer: ([SHOW ANSWER](#))

Frequent system backups (B) are the most effective means of recovery from ransomware or malware attacks.

CISM emphasizes resilience and recoverability as critical aspects of incident management. While incident response plans (A), antivirus updates (C), and awareness training (D) help prevent or manage incidents, they do not guarantee restoration of data or systems. Reliable, tested backups

allow organizations to restore operations without paying ransoms or suffering permanent data loss.

References: ISACA CISM Review Manual (Incident management-recovery and resilience); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 338

When developing security processes for handling credit card data on the business unit's information system, the information security manager should FIRST:

- A. review corporate policies regarding credit card information.
- B. ensure alignment with industry encryption standards.
- C. ensure that systems that handle credit card data are segmented.
- D. review industry best practices for handling secure payments.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 339

An organization is in the process of defining policies for employee use of social media. It is MOST important for the information security manager to:

- A. Assign accountability for monitoring social media
- B. Identify security monitoring tools
- C. Evaluate risks to the organization
- D. Develop security awareness training

Answer: ([SHOW ANSWER](#))

Before drafting or enforcing policies, the first step is to evaluate the risks posed by employee use of social media. This may include data leakage, reputational damage, phishing, and legal liability. Once risks are identified and understood in the organization's context, policies can be developed that specifically address those risks. Acting prematurely without a risk assessment can lead to overly restrictive or insufficient policies.

"Security policies should be risk-driven. Understanding potential threats and impacts is the foundation for effective policy creation."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Risk-Based Policy Development*

NEW QUESTION: 340

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 efficiency of information security processes and activities. They help senior management 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 objectives. KPIs can also be used to benchmark the organization's security performance against industry

standards or best practices. KPIs should be aligned with the organization's strategic goals and risk appetite, and should be reported regularly to senior management 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: 341

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: 342

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: 343

Which of the following would BEST support the business case for an increase in the information security budget?

- A. Cost-benefit analysis results
- B. Comparison of information security budgets with peer organizations
- C. Business impact analysis (BIA) results
- D. Frequency of information security incidents

Answer: (SHOW ANSWER)

Cost-benefit analysis results are the best way to support the business case for an increase in the information security budget because they help to demonstrate the value and return on investment of the proposed security initiatives or projects. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or options, taking into account both quantitative and qualitative factors. A cost-benefit analysis helps to justify the need and feasibility of the security budget, as well as to prioritize the security spending based on the expected outcomes and impacts. Therefore, cost-benefit analysis results are the correct answer.

References:

<https://www.cisa.gov/resources-tools/resources/business-case-security>

<https://www.cisa.gov/resources-tools/resources/isc-best-practices-making-business-case-security>

<https://risk3sixty.com/2020/09/21/how-to-build-a-business-case-for-security-initiatives-part-4/>

NEW QUESTION: 344

An organization is leveraging tablets to replace desktop computers shared by shift-based staff. These tablets contain critical business data and are inherently at increased risk of theft. Which of the following will BEST help to mitigate this risk?

- A. Deploy mobile device management (MDM)
- B. Implement remote wipe capability.
- C. Create an acceptable use policy.
- D. Conduct a mobile device risk assessment

Answer: (SHOW ANSWER)

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For

example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. References:

<https://www.isaca.org/credentialing/cism> <https://www.wiley.com/en-us>

/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 345

Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?

- A. Providing training from third-party forensics firms
- B. Obtaining industry certifications for the response team
- C. Conducting tabletop exercises appropriate for the organization
- D. Documenting multiple scenarios for the organization and response steps

Answer: (SHOW ANSWER)

The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.

Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.

According to the Certified Information Security Manager (CISM) Study Manual, "Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan." While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

NEW QUESTION: 346

Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?

- A. Security metrics
- B. Security baselines
- C. Security incident details
- D. Security risk exposure

Answer: A (LEAVE A REPLY)

Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.

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.

The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 347

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, objectives, 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 organization's assets, as well as the potential impact and likelihood

of incidents. A security policy should also be aligned with the organization's business objectives and risk appetite¹. 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 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. 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 organizations, 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 devices 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 granular 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 Management - ISACA 3: Deploy and manage Removable Storage Access Control using Intune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Removable Media Policy Writing Tips - CurrentWare

NEW QUESTION: 348

Which of the following has the GREATEST impact on efforts to improve an organization's security posture?

- A. Regular reporting to senior management
- B. Supportive tone at the top regarding security
- C. Automation of security controls
- D. Well-documented security policies and procedures

Answer: ([SHOW ANSWER](#))

The supportive tone at the top regarding security is the greatest impact on efforts to improve an organization's security posture. This means that senior management should demonstrate their commitment and leadership to information security by setting clear goals, allocating adequate resources, communicating effectively, and rewarding good practices. A supportive tone at the top can also influence the culture and behavior of the organization, as well as foster trust and collaboration among stakeholders¹². References = CISM Review Manual 15th Edition, page 1261; CISM Item Development Guide, page 82

NEW QUESTION: 349

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: ([SHOW ANSWER](#))

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: 350

An organization is in the process of acquiring a new company. Which of the following is the FIRST step to determine how to protect newly acquired data assets prior to integration?

- A. Inventory information assets
- B. Include security requirements in the contract
- C. Assess security controls
- D. Review data architecture

Answer: (SHOW ANSWER)

The correct answer is A because the organization must first identify and inventory the newly acquired information assets before determining how to protect them. Without knowing what data assets exist, where they are located, who owns them, how they are used, and what sensitivity or criticality they have, the organization cannot select appropriate controls. Including security requirements in the contract is important during acquisition planning, but the question asks how to protect newly acquired data assets prior to integration. Assessing controls is necessary, but it should be based on a clear understanding of the assets being protected. Reviewing data architecture is useful, but it is also dependent on first identifying the assets and their locations. CISM risk management emphasizes asset identification, ownership, classification, and risk assessment as foundational steps in protecting information. An asset inventory enables classification, impact analysis, access review, control selection, and integration planning. Therefore, inventorying information assets is the correct first step.

Reference: CISM Information Risk Management; asset inventory, information classification, acquisition risk, and data protection planning principles.

NEW QUESTION: 351

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 audit a 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: 352

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: 353

Reevaluation of risk is MOST critical when there is:

- A. resistance to the implementation of mitigating controls.
- B. a management request for updated security reports.
- C. a change in security policy.
- D. a change in the threat landscape.

Answer: (SHOW ANSWER)

= Reevaluation of risk is a vital aspect of the risk management process that helps organizations to identify and analyze new or evolving threats, vulnerabilities, and impacts on their assets, and implement the necessary controls to mitigate them. Reevaluation of risk is most critical when there is a change in the threat landscape, which refers to the external and internal factors that influence the likelihood and severity of potential attacks on the organization's information assets. A change in the threat landscape may be caused by various factors, such as technological innovations, geopolitical events, cybercrime trends, regulatory changes, or organizational changes. A change in the threat landscape may introduce new risks or alter the existing risk

profile of the organization, requiring a reassessment of the risk appetite, tolerance, and strategy. Reevaluation of risk helps the organization to adapt to the changing threat landscape and ensure that the information security program remains effective, efficient, and aligned with the business objectives.

References =

- * CISM Review Manual 15th Edition, page 1131
- * CISM Domain 2: Information Risk Management (IRM) [2022 update]²
- * Reevaluation of Risk | CISM Exam Question Answer | ISACA³

NEW QUESTION: 354

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. infosecrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

NEW QUESTION: 355

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?

- 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: 356

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: 357

An information security manager is alerted to multiple security incidents across different business units, with unauthorized access to sensitive data and potential data exfiltration from critical systems. Which of the following is the BEST course of action to appropriately classify and prioritize these incidents?

- A. Assemble the incident response team to evaluate the incidents
- B. Initiate the crisis communication plan to notify stakeholders of the incidents
- C. Engage external incident response consultants to conduct an independent investigation
- D. Prioritize the incidents based on data classification standards

Answer: (SHOW ANSWER)

Prioritizing incidents based on data classification standards ensures that the most sensitive and critical data exposures are addressed first, reducing the potential impact on the business.

"The impact of incidents should be evaluated based on the classification and sensitivity of the data involved."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization* ISACA practice questions emphasize the importance of using data classification to properly prioritize incident response efforts.

NEW QUESTION: 358

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. Transfer the risk by purchasing insurance.
- C. Accept the risk, as the benefits exceed the potential consequences.
- D. Mitigate the risk by applying anonymization on the data set.

Answer: (SHOW ANSWER)

NEW QUESTION: 359

An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?

- A. Identify the skill set of the provider's incident response team.
- B. Evaluate the provider's audit logging and monitoring controls.

C. Review the provider's incident definitions and notification criteria.

D. Update the incident escalation process.

Answer: (SHOW ANSWER)

When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. References = CISM Review Manual, 16th Edition, page 1021 Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

NEW QUESTION: 360

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: A (LEAVE A REPLY)

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: 361

When drafting the corporate privacy statement for a public website, which of the following **MUST** be included?

- A. Limited liability clause
- B. Explanation of information usage
- C. Information encryption requirements
- D. Access control requirements

Answer: (SHOW ANSWER)

A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 362

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: 363

The **PRIMARY** purpose for continuous monitoring of security controls is to ensure:

- A. control gaps are minimized.
- B. system availability.
- C. effectiveness of controls.

D. alignment with compliance requirements.

Answer: ([SHOW ANSWER](#))

The primary purpose for continuous monitoring of security controls is to ensure the effectiveness of controls.

This involves regularly assessing the controls to ensure that they are meeting their intended objectives, and that any potential weaknesses are identified and addressed. Continuous monitoring also helps to ensure that control gaps are minimized, and that systems are available and aligned with compliance requirements.

The primary purpose of continuous monitoring of security controls is to ensure that the controls are operating effectively and providing adequate protection for the information assets. Continuous monitoring can also help to identify control gaps, ensure system availability, and support compliance requirements, but these are secondary benefits¹² References = 1: SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, page 1-12: A Practical Approach to Continuous Control Monitoring, ISACA Journal, Volume 2, 2015, page 1.

NEW QUESTION: 364

An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

- A.** Red team exercise
- B.** Black box penetration test
- C.** Disaster recovery exercise
- D.** Tabletop exercise

Answer: **D** ([LEAVE A REPLY](#))

= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low- cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.

A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature

and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A disaster recovery exercise is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high-risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

NEW QUESTION: 365

Which of the following would BEST enable a new information security manager to assess the current state of information security governance within the organization?

- A.** Conducting a business impact analysis (BIA) to understand business priorities
- B.** Analyzing the integration of information security policies and practices within business processes
- C.** Performing both quantitative and qualitative risk analyses
- D.** Interviewing key personnel identified within the governance framework

Answer: ([SHOW ANSWER](#))

Analyzing how security policies and practices are integrated into business processes (B) provides the clearest view of governance effectiveness. CISM defines governance as the alignment of security with business objectives, supported by defined roles, accountability, and decision-making structures. BIAs (A) and risk analyses (C) provide valuable inputs but do not directly assess governance maturity. Interviews (D) can supplement understanding but are subjective without observing real integration. By evaluating whether security is embedded in procurement, development, operations, and decision workflows, a new security manager can determine whether governance is formalized, consistently applied, and supported by management.

References: ISACA CISM Review Manual (Governance-structure, integration, and effectiveness); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 366

An anomaly-based intrusion detection system (IDS) operates by gathering data on:

- A. normal network behavior and using it as a baseline for measuring abnormal activity
- B. abnormal network behavior and issuing instructions to the firewall to drop rogue connections
- C. abnormal network behavior and using it as a baseline for measuring normal activity
- D. attack pattern signatures from historical data

Answer: (SHOW ANSWER)

An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

NEW QUESTION: 367

Which of the following is MOST helpful in determining the criticality of an organization's business functions?

- A. Disaster recovery plan (DRP)
- B. Business impact analysis (BIA)
- C. Business continuity plan (BCP)
- D. Security assessment report (SAR)

Answer: (SHOW ANSWER)

Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.

References:

<https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez>

<https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business-continuity-Understanding-impact-criticality>

NEW QUESTION: 368

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: D ([LEAVE A REPLY](#))

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: 369

Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?

- A. Projected Increase in maturity level
- B. Estimated reduction in risk
- C. Projected costs over time
- D. Estimated increase in efficiency

Answer: ([SHOW ANSWER](#)**)**

The best thing to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its cost-effectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity

and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

NEW QUESTION: 370

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: ([SHOW ANSWER](#))

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: 371

Which of the following is the GREATEST inherent risk when performing a disaster recovery plan (DRP) test?

- A. Poor documentation of results and lessons learned
- B. Lack of communication to affected users
- C. Disruption to the production environment
- D. Lack of coordination among departments

Answer: ([SHOW ANSWER](#))

A disaster recovery plan (DRP) test is a simulation of a disaster scenario to evaluate the effectiveness and readiness of the DRP. The greatest inherent risk when performing a DRP test is the disruption to the production environment, which could cause operational issues, data loss, or system damage. Therefore, it is essential to plan and execute the DRP test carefully, with proper backup, isolation, and rollback procedures.

Poor documentation, lack of communication, and lack of coordination are also potential risks, but they are not as severe as disrupting the production environment. References = CISM Review Manual 15th Edition, page

253; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 224.

The greatest inherent risk when performing a disaster recovery plan (DRP) test is disruption to the production environment. A DRP test involves simulating a disaster scenario to ensure that the organization's plans are effective and that it is able to recover from an incident. However, this involves running tests on the production environment, which has the potential to disrupt the normal operations of the organization. This inherent risk can be mitigated by running tests on a non-production environment or by running tests at times when disruption will be minimized.

NEW QUESTION: 372

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: 373

Which of the following is the PRIMARY objective of the incident management recovery phase?

- A. To recover business operation support
- B. To perform a lessons-learned review
- C. To document actions taken to restore IT systems
- D. To bring IT services back online

Answer: ([SHOW ANSWER](#))

The correct answer is D because the recovery phase focuses on restoring affected IT services, systems, and operations after containment and eradication have been completed. The objective

is to return services to an operational state in a controlled manner while ensuring that the threat has been removed and systems are stable. Recovering business operation support is related to the broader business continuity goal, but the recovery phase of incident management is primarily concerned with restoring IT services and affected environments. Performing a lessons-learned review usually occurs after recovery, during post-incident review or improvement activities. Documenting restoration actions is important for evidence, accountability, and future analysis, but documentation is not the primary objective of recovery. In CISM incident management, recovery includes restoring systems, validating functionality, monitoring for recurrence, and returning operations to normal. Therefore, the primary objective of the recovery phase is to bring IT services back online safely and effectively.

Reference: CISM Information Security Incident Management; recovery phase, service restoration, post-incident activities, and operational resilience principles.

NEW QUESTION: 374

Management has announced the acquisition of a new company. The information security manager of the parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies. To BEST address this concern, the information security manager should:

- A.** review access rights as the acquisition integration occurs.
- B.** perform a risk assessment of the access rights.
- C.** escalate concerns for conflicting access rights to management.
- D.** implement consistent access control standards.

Answer: (SHOW ANSWER)

Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls¹. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. References: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful post-merger integration

NEW QUESTION: 375

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: B ([LEAVE A REPLY](#))

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: 376

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

- A. Perform a risk assessment
- B. Perform a gap analysis
- C. Review information security policies
- D. Review the state of security awareness

Answer: A ([LEAVE A REPLY](#))

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.

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

NEW QUESTION: 377

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?

- A. To prevent accountability issues
- B. To ensure system audit trails are not bypassed
- C. To ensure separation of duties is maintained
- D. To prevent unauthorized user access

Answer: (SHOW ANSWER)

NEW QUESTION: 378

Which of the following is the MOST important outcome of a post-incident review?

- A. The impact of the incident is reported to senior management.
- B. The system affected by the incident is restored to its prior state.
- C. The person responsible for the incident is identified.
- D. The root cause of the incident is determined.

Answer: (SHOW ANSWER)

Determining the root cause of the incident is essential for preventing or minimizing the recurrence of similar incidents, as well as for identifying and implementing corrective actions to improve the security posture of the organization.

References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.3

NEW QUESTION: 379

When mitigation is the chosen risk treatment, which of the following roles is responsible for effective implementation of the chosen treatment?

- A. Risk owner
- B. Control owner
- C. Business system owner
- D. Application owner

Answer: (SHOW ANSWER)

The control owner is the individual accountable for implementing and managing specific controls that mitigate risks. While the risk owner is responsible for the overall risk and decision-making, it

is the control owner who ensures the selected mitigation is effectively implemented and maintained.

"The control owner is responsible for ensuring that the control is properly designed, implemented, and operating effectively."

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

ISACA practice questions stress this distinction: the control owner is tasked with the execution of mitigation strategies.

NEW QUESTION: 380

An information security manager is considering options for protecting the data on a web-facing legacy application that cannot be patched. Which of the following would provide the BEST information about the effectiveness of compensating controls?

- A. Threat assessment
- B. Intrusion detection system logs
- C. Penetration testing
- D. Firewall rules

Answer: ([SHOW ANSWER](#))

The correct answer is C because penetration testing provides practical evidence of whether compensating controls can resist real-world attack techniques against the legacy application. When an application cannot be patched, compensating controls such as web application firewalls, network segmentation, access restrictions, monitoring, or virtual patching may be used to reduce risk. However, the effectiveness of those controls should be validated through testing that simulates attacker behavior. A threat assessment identifies potential threats, but it does not prove whether controls are working. Intrusion detection system logs may show detected activity, but they provide only a partial and reactive view. Firewall rules can be reviewed, but rule review alone does not demonstrate whether the total control environment prevents exploitation. Penetration testing is more useful because it tests the application and compensating controls together under realistic conditions. CISM emphasizes risk-based control validation, especially where vulnerabilities cannot be remediated directly. Therefore, penetration testing provides the best information about compensating control effectiveness.

Reference: CISM Information Risk Management; compensating controls, vulnerability management, penetration testing, and control effectiveness principles.

NEW QUESTION: 381

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: 382

Which of the following is an information security manager's BEST recommendation to senior management following a breach at the organization's Software as a Service (SaaS) vendor?

- A.** Terminate the relationship with the vendor.
- B.** Renegotiate the vendor contract.
- C.** Update the vendor risk assessment.
- D.** Engage legal counsel.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 383

Which of the following BEST enables the integration of information security governance into corporate governance?

- A.** Well-documented information security policies and standards
- B.** An information security steering committee with business representation
- C.** Clear lines of authority across the organization
- D.** Senior management approval of the information security strategy

Answer: ([SHOW ANSWER](#)**)**

= The best way to enable the integration of information security governance into corporate governance is to establish an information security steering committee with business representation. An information security steering committee is a group of senior executives and managers from different business units and functions who are responsible for overseeing, directing, and supporting the information security program and strategy of the organization. An information security steering committee with business representation can enable the integration of information security governance into corporate governance by providing the following benefits¹²: Align the information security objectives and priorities with the business objectives and priorities, and ensure that the information security program and strategy support and enable the achievement of the organizational goals and performance.

Communicate and promote the value and importance of information security to the board of directors, senior management, and other stakeholders, and ensure that information security is considered and incorporated in the decision making and planning processes of the organization. Provide guidance and direction to the information security manager and the information security team, and ensure that they have the necessary authority, resources, and support to implement and maintain the information security program and strategy effectively and efficiently.

Monitor and evaluate the performance and outcomes of the information security program and strategy, and ensure that they are aligned with the expectations and requirements of the

organization and its stakeholders, as well as the relevant laws, regulations, standards, and best practices.

Identify and address the issues, challenges, and opportunities related to information security, and ensure that the information security program and strategy are continuously improved and updated to reflect the changes and developments in the internal and external environment.

The other options are not the best way to enable the integration of information security governance into corporate governance, as they are less comprehensive, effective, or influential than establishing an information security steering committee with business representation. Well-documented information security policies and standards are important components of the information security program and strategy, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not reflect or align with the business needs, priorities, or expectations, and they may not be communicated, implemented, or enforced properly or consistently across the organization. Clear lines of authority across the organization are important factors for the information security governance structure, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not ensure the involvement, participation, or support of the senior executives, managers, and other stakeholders who are responsible for or affected by information security. Senior management approval of the information security strategy is an important outcome of the information security governance process, but it is not sufficient to enable the integration of information security governance into corporate governance, as it may not ensure the alignment, communication, or monitoring of the information security strategy with the business strategy, and it may not ensure the accountability, responsibility, or authority of the information security manager and the information security team¹². References = CISM Domain 1: Information Security Governance (ISG) [2022 update], Information Security Governance for CISM | Pluralsight, Aligning Information Security with Business Strategy - ISACA, Aligning Information Security with Business Objectives - ISACA

NEW QUESTION: 384

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.csoononline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html>

NEW QUESTION: 385

Which of the following is the MOST important consideration when establishing an organization's information security governance committee?

- A.** Members have knowledge of information security controls.
- B.** Members are business risk owners.
- C.** Members are rotated periodically.
- D.** Members represent functions across the organization.

Answer: D (LEAVE A REPLY)

= The most important consideration when establishing an organization's information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization's business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization's mission, vision, and values. Having a diverse and representative committee also helps to foster a culture of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.

Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization's business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization's business objectives, and to allocate appropriate resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the

organization's information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee's ability to monitor and evaluate the performance and progress of the information security program. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37. ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1014.

NEW QUESTION: 386

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: (SHOW ANSWER)

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)

NEW QUESTION: 387

A global organization is planning to expand its operations into a new country with stricter data protection regulations than those in the headquarters' home country. Which of the following is the BEST approach for adopting these new requirements?

- A. Ensure local operations comply with geographical data protection laws of the headquarters.

- B.** Procure cybersecurity insurance that covers potential breaches and incidents in the new country.
- C.** Work with legal to interpret the local regulatory requirements and implement applicable controls.
- D.** Adjust organization-wide security policies to align with regulations of the new country.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 388

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: 389

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: 390

Which of the following is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

- A. To reduce the overall cost of policy development
- B. To share responsibility for addressing security breaches
- C. To decrease the workload of the IT department
- D. To gain acceptance of the policy across the organization

Answer: ([SHOW ANSWER](#))

The main reason to involve stakeholders from various business units is to gain their acceptance and buy-in for the information security policy. The CISM Review Manual underlines that policies are more effective and enforceable when stakeholders understand and agree with them, which also aids in smooth policy implementation across the organization.

Reference:ISACA CISM Review Manual, 16th Edition, Page 45, "Stakeholder Involvement in Policy Development".

NEW QUESTION: 391

Which of the following should the information security manager do FIRST after a ransomware attack is confirmed?

- A. Perform hardening of the affected endpoints
- B. Rebuild the affected endpoints
- C. Restore data backup from the cloud
- D. Isolate the impacted endpoints

Answer: ([SHOW ANSWER](#))

The correct answer is D because once a ransomware attack is confirmed, the immediate priority is containment. Isolating impacted endpoints helps prevent the ransomware from spreading to additional systems, encrypting shared drives, communicating with command-and-control infrastructure, or causing further business disruption. Hardening affected endpoints is important later to reduce recurrence, but it is not the first action during an active ransomware incident.

Rebuilding endpoints may be required after containment and investigation, but doing so immediately could destroy evidence and may not stop spread if other systems remain infected. Restoring backups should occur only after containment, eradication, and validation that the environment is safe; otherwise, restored data may be encrypted again. CISM incident management principles prioritize detection, validation, containment, eradication, recovery, and lessons learned. Since the ransomware attack is already confirmed, the first action must be to limit impact and stop propagation. Therefore, isolating impacted endpoints is the correct answer. Reference: CISM Information Security Incident Management; ransomware response, containment, endpoint isolation, eradication, and recovery principles.

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

NEW QUESTION: 392

Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?

- A. Create a security exception.
- B. Perform a gap analysis to determine needed resources.
- C. Perform a vulnerability assessment.
- D. Assess the risk to business operations.

Answer: (SHOW ANSWER)

The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.

References = CISM Review Manual, 16th Edition, page 48

NEW QUESTION: 393

Which type of test is MOST effective in communicating the roles of end users to support timely identification and response to information security incidents?

- A. Parallel
- B. Complete failover
- C. Checklist
- D. Walkthrough

Answer: ([SHOW ANSWER](#))

The correct answer is D because a walkthrough test is well suited for explaining and validating roles, responsibilities, communication flows, and expected actions among participants, including end users. In an incident response context, end users often play an important role in identifying suspicious activity, reporting incidents quickly, avoiding further damage, and following escalation instructions. A walkthrough allows participants to step through a scenario and discuss what actions should be taken at each stage. This makes it effective for communicating responsibilities and improving understanding. A parallel test is more commonly associated with running alternate processes or systems alongside normal operations. A complete failover test is more technical and disruptive, typically used for disaster recovery or continuity validation. A checklist test may confirm whether documented items exist, but it is less effective for communicating practical roles and expectations. CISM emphasizes awareness, training, testing, and role clarity as key enablers of timely incident identification and response.

Reference: CISM Information Security Incident Management; incident response testing, walkthrough exercises, user awareness, and role communication principles.

NEW QUESTION: 394

Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

- A. Monitor the effectiveness of controls
- B. Update the risk assessment framework
- C. Review the inherent risk level
- D. Review the risk probability and impact

Answer: ([SHOW ANSWER](#))

If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

NEW QUESTION: 395

Which of the following is the MOST effective way to detect information security incidents?

- A. Periodic analysis of security event log records
- B. Real-time monitoring of network activity
- C. Threshold settings on key risk indicators (KRIs)
- D. Implementation of regular security awareness programs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 396

Conducting log analysis falls into which phase of the incident management life cycle?

- A. Post-incident
- B. Containment
- C. Detection
- D. Planning

Answer: ([SHOW ANSWER](#))

Log analysis is a core detection activity (C) within the incident management lifecycle. Logs provide evidence of abnormal activity, policy violations, or indicators of compromise that enable security teams to identify potential incidents. While logs may also be reviewed during post-incident analysis, their primary role in the lifecycle is to detect events and trigger incident response. Containment (B) focuses on limiting damage after an incident is confirmed, and planning (D) involves preparation activities such as procedures and roles. CISM emphasizes strong detection capabilities-including log monitoring, SIEM, and alerting-as essential to reducing mean time to detect (MTTD) and limiting business impact.

References: ISACA CISM Review Manual (Incident management-lifecycle phases, detection and monitoring); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 397

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: 398

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: 399

An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?

- A. Install the OS, patches, and application from the original source.
- B. Restore the OS, patches, and application from a backup.

- C. Restore the application and data from a forensic copy.
- D. Remove all signs of the intrusion from the OS and application.

Answer: (SHOW ANSWER)

After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.

References =

* ISACA, CISM Review Manual, 16th Edition, 2020, page 2401

* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132 The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

NEW QUESTION: 400

Which of the following is the responsibility of a risk owner?

- A. Implementing risk treatment plan activities with control owners
- B. Evaluating control effectiveness
- C. Approving risk treatment plans
- D. Approving the selection of risk mitigation measures

Answer: C (LEAVE A REPLY)

A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk.

While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

NEW QUESTION: 401

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?

- A. Integrity
- B. Authenticity
- C. Confidentiality
- D. Nonrepudiation

Answer: ([SHOW ANSWER](#))

Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References:
<https://www.csoononline.com/article/3513899/the-cia-triad-definition-components-and-examples.html>

NEW QUESTION: 402

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. Automate user provisioning activities.
- B. Implement monitoring of IT administrator activities.
- C. Maintain strict control over user provisioning activities.
- D. Formally document IT administrator activities.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 403

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: 404

Which of the following is MOST important when designing an information security governance framework?

- A. Assessing the availability of information security resources
- B. Assessing the current state of information security
- C. Aligning with the information security strategy
- D. Aligning with industry best practice frameworks

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 405

Which of the following would provide the MOST effective security outcome in an organizations contract management process?

- A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage
- B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage
- C. Extending security assessment to cover asset disposal on contract termination
- D. Extending security assessment to include random penetration testing

Answer: ([SHOW ANSWER](#))

Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance.

Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. References: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud>

<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions>

NEW QUESTION: 406

Which of the following is the BEST indicator of a successful intrusion into an organization's systems?

- A. Increase in the number of failed login attempts
- B. Decrease in internal network traffic
- C. Decrease in available storage space
- D. Increase in the number of irregular application requests

Answer: ([SHOW ANSWER](#))

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: [freecram](#))

NEW QUESTION: 407

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: 408

What should a global information security manager do FIRST when informed that a new regulation with significant impact will go into effect soon?

- A. Perform a gap analysis.
- B. Perform a privacy impact assessment (PIA).
- C. Perform a vulnerability assessment.
- D. Perform a business impact analysis (BIA).

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 409

Which of the following is the PRIMARY role of the information security manager in application development?

- A. To ensure security is integrated into the system development life cycle (SDLC)
- B. To ensure compliance with industry best practice
- C. To ensure enterprise security controls are implemented
- D. To ensure control procedures address business risk

Answer: ([SHOW ANSWER](#))

According to the CISM Review Manual, one of the primary roles of the information security manager in application development is to ensure that security is integrated into the SDLC. This means that security requirements, design, testing, deployment, and maintenance are all considered and addressed throughout the application development process. By doing so, the information security manager can help to prevent or mitigate security risks, ensure compliance with standards and regulations, and improve the quality and reliability of the application¹ The other options are not as accurate as ensuring security is integrated into the SDLC. Ensuring compliance with industry best practices is a secondary role of the information security manager in application development, as it involves following established guidelines and frameworks for secure application development. However, compliance alone does not guarantee that security is actually implemented in the application. Ensuring enterprise security controls are implemented is a tertiary role of the information security manager in application development, as it involves applying existing policies and procedures for managing and monitoring security activities across the organization. However, enterprise controls alone do not ensure that security is tailored to the specific needs and context of each application. Ensuring control procedures address business risk is a quaternary role of the information security manager in application development, as it involves identifying and assessing potential threats and vulnerabilities that could affect the business objectives and operations of each application. However, business risk alone does not

ensure that security measures are aligned with the value proposition and benefits of each application1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 30-31...

NEW QUESTION: 410

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: 411

Which of the following is the BEST indicator of the maturity level of a vendor risk management process?

- A. Average time required to complete the vendor risk management process
- B. Percentage of vendors that have gone through the vendor onboarding process
- C. Percentage of vendors that are regularly reviewed against defined criteria
- D. Number of vendors rejected because of security review results

Answer: (SHOW ANSWER)

The percentage of vendors that are regularly reviewed against defined criteria is the best indicator of the maturity level of a vendor risk management process, as it reflects the extent to which the organization has established and implemented a consistent, repeatable, and effective process to monitor and evaluate the security performance and compliance of its vendors. A high percentage indicates a mature process that covers all vendors and applies clear and relevant criteria based on the organization's risk appetite and objectives. A low percentage indicates a less mature process that may be ad hoc, incomplete, or outdated. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 412

Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

- A. Threat management is enhanced.
- B. Compliance status is improved.
- C. Security metrics are enhanced.
- D. Proactive risk management is facilitated.

Answer: (SHOW ANSWER)

A vulnerability assessment process is a systematic and proactive approach to identify, analyze and prioritize the vulnerabilities in an information system. It helps to reduce the exposure of the system to potential threats and improve the security posture of the organization. By implementing a vulnerability assessment process, the organization can facilitate proactive risk management, which is the PRIMARY benefit of this process.

Proactive risk management is the process of identifying, assessing and mitigating risks before they become incidents or cause significant impact to the organization. Proactive risk management enables the organization to align its security strategy with its business objectives, optimize its security resources and investments, and enhance its resilience and compliance.

A). Threat management is enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Threat management is the process of identifying, analyzing and responding to the threats that may exploit the vulnerabilities in an information system. Threat management is enhanced by implementing a vulnerability assessment process, as it helps to reduce the attack surface and prioritize the most critical threats.

However, threat management is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a reactive rather than proactive approach to risk management.

B). Compliance status is improved. This is a secondary benefit of implementing a vulnerability assessment process. Compliance status is the degree to which an organization adheres to the applicable laws, regulations, standards and policies that govern its information security.

Compliance status is improved by implementing a vulnerability assessment process, as it helps to demonstrate the organization's commitment to security best practices and meet the expectations of the stakeholders and regulators. However, compliance status is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a result rather than a driver of risk management.

C). Security metrics are enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Security metrics are the quantitative and qualitative measures that indicate the effectiveness and efficiency of the information security processes and controls. Security metrics are enhanced by implementing a vulnerability assessment process, as it helps to provide objective and reliable data for security monitoring and reporting. However, security metrics are not the PRIMARY benefit of implementing a vulnerability assessment process, as they are a means rather than an end of risk management.

References =

* CISM Review Manual 15th Edition, pages 1-301

* CISM Exam Content Outline2

- * Risk Assessment for Technical Vulnerabilities³
- * A Step-By-Step Guide to Vulnerability Assessment⁴

NEW QUESTION: 413

Detailed business continuity plans (BCPs) should be PRIMARILY based on:

- A. strategies validated by senior management.
- B. cost and resources needed to execute.
- C. strategies that cover all applications.
- D. capabilities of available local vendors.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 414

Which of the following is MOST important for the successful implementation of an incident response plan?

- A. Developing metrics for incident response reporting
- B. Ensuring response staff are appropriately trained
- C. Developing a RACI chart of response staff functions
- D. Establishing an escalation process for the help desk

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 415

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: 416

It is MOST important that risk owners understand they are accountable for:

- A. Reporting risk metrics and control compliance status to the information security manager
- B. Escalating control deficiencies associated with the risk to the steering committee for decision making

C. Collaborating with stakeholders to evaluate the effectiveness of controls associated with the risk

D. Overseeing and monitoring the effectiveness of controls associated with the risk

Answer: (SHOW ANSWER)

It is most important that risk owners understand they are accountable for overseeing and monitoring the effectiveness of controls associated with the risk. In CISM, risk ownership means accountability for managing a risk within the organization's risk appetite. The risk owner does not necessarily operate every control, but must ensure that appropriate treatment is selected, controls are effective, residual risk is understood, and issues are addressed. Reporting metrics to the information security manager is useful, but it is only part of oversight and does not fully define accountability. Escalating deficiencies may be required when risks exceed tolerance, but escalation alone is not the primary accountability. Collaborating with stakeholders is important, but accountability remains with the risk owner. CISM separates control ownership from risk ownership: control owners may operate controls, while risk owners remain accountable for the business risk and outcomes. Therefore, overseeing and monitoring the effectiveness of related controls is the most important accountability for risk owners.

References:

ISACA CISM Review Manual, Information Risk Management - risk ownership, control monitoring, and accountability ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

NEW QUESTION: 417

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

NEW QUESTION: 418

Which of the following is MOST important for guiding the development and management of a comprehensive information security program?

- A. Adopting information security program management best practices
- B. Implementing policies and procedures to address the information security strategy
- C. Aligning the organization's business objectives with IT objectives
- D. Establishing and maintaining an information security governance framework

Answer: D ([LEAVE A REPLY](#))

An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified. References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 419

Which of the following incident response phases involves actions to help safeguard critical systems while maintaining business operations?

- A. Recovery
- B. Identification
- C. Containment
- D. Preparation

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 420

For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:

- A. consistent security.
- B. comprehensive audits
- C. a security-aware culture
- D. compliance with policy

Answer: A ([LEAVE A REPLY](#))

Consistent security is the primary reason for integrating the various assurance functions of an organization for the information security manager because it ensures that the security policies and standards are applied uniformly and effectively across different domains, processes, and systems of the organization.

Comprehensive audits are not the primary reason for integrating the various assurance functions, but rather a possible outcome or benefit of doing so. A security-aware culture is not the primary reason for integrating the various assurance functions, but rather a desirable state or goal of the organization. Compliance with policy is not the primary reason for integrating the various assurance functions, but rather a basic requirement or expectation of the organization.

References: <https://www.isaca.org/resources/isaca-journal/issues/2016>

/volume-4/integrating-assurance-functions <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system>

NEW QUESTION: 421

Which of the following tools would be MOST helpful to an incident response team?

- A. Intrusion detection system (IDS)
- B. Endpoint detection and response (EDR) solution
- C. User and entity behavior analytics
- D. Vulnerability scanning tools

Answer: (SHOW ANSWER)

An endpoint detection and response (EDR) solution provides advanced visibility, detection, and response capabilities at the endpoint level, which are critical for investigating and responding to incidents.

"EDR solutions help identify, investigate, and respond to threats on endpoints quickly, making them vital for incident response teams."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Tools and Technologies for Incident Response* ISACA's practice questions highlight EDR as the most helpful tool for comprehensive incident analysis and response.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 422

Which of the following is MOST useful to an information security manager when reporting the performance of the information security program to senior management?

- A. Number of policy exceptions
- B. Number of incidents identified and remediated
- C. System vulnerability scan results
- D. Results of an independent security audit

Answer: (SHOW ANSWER)

The correct answer is D because an independent security audit provides objective assurance about the performance and effectiveness of the information security program. Senior management needs reliable, high-level information to evaluate whether the program is achieving its objectives, managing risk appropriately, and supporting business goals. An independent audit

can assess governance, controls, compliance, risk management, operations, and program maturity from an unbiased perspective. The number of policy exceptions is useful as a metric, but it gives only a narrow view of compliance behavior. The number of incidents identified and remediated may show operational activity, but it does not fully measure program effectiveness. Vulnerability scan results are technical and limited to specific systems or environments; they do not provide an enterprise-level view of program performance. CISM governance emphasizes management reporting, independent assurance, accountability, and performance evaluation. Therefore, among the listed options, independent security audit results are the most useful for reporting overall program performance to senior management.

Reference: CISM Information Security Governance; program reporting, independent assurance, audit results, and senior management oversight principles.

NEW QUESTION: 423

An information security manager is concerned with continued security policy violations in a particular business unit despite recent efforts to rectify the situation. What is the BEST course of action?

- A.** Enforce sanctions on the business unit.
- B.** Revise the policy to accommodate the business unit.
- C.** Report the business unit for policy noncompliance.
- D.** Review the business unit's function against the policy.

Answer: (SHOW ANSWER)

The best course of action is to review the business unit's function against the policy (D). According to CISM governance principles, persistent policy violations often indicate a misalignment between policy requirements and business operations, rather than willful noncompliance. CISM emphasizes that information security policies must be aligned with business objectives, operational realities, and risk appetite to be effective and enforceable. Before escalating to sanctions (A) or reporting noncompliance (C), the information security manager should determine whether the policy is clearly understood, practical to implement, and supported by appropriate standards and procedures. Revising the policy to accommodate violations (B) without analysis weakens governance and may increase risk. By reviewing the business unit's function against the policy, the security manager can identify root causes such as unclear requirements, missing procedures, inadequate training, or legitimate business constraints requiring approved exceptions or compensating controls.

CISM stresses a root-cause and business-aligned approach to governance issues, ensuring that enforcement actions are justified, proportional, and supported by management intent.

References:

ISACA CISM Review Manual, Information Security Governance - policy alignment, enforcement, and exception management
ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 424

An information security manager has become aware that system administrators are not changing server administrator accounts from the default usernames. A policy has been created and approved by business managers to require these changes. Which of the following should be the information security manager's FIRST course of action?

- A. Include the requirement in information security awareness materials
- B. Perform a policy compliance assessment
- C. Ensure the policy has been communicated to the system administrators

Answer: ([SHOW ANSWER](#))

The first course of action is to ensure the policy has been communicated to the system administrators (C).

CISM governance principles require that policies be formally communicated and understood before enforcement or compliance assessment occurs. Conducting assessments (B) or training (A) is ineffective if administrators are not aware of the policy requirements. Effective governance follows a sequence: approval # communication # implementation # monitoring and enforcement. Communication ensures accountability and supports consistent adoption of security requirements.

References: ISACA CISM Review Manual (Governance-policy lifecycle, communication and enforcement); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 425

Which type of plan is PRIMARILY intended to reduce the potential impact of security events that may occur?

- A. Security awareness plan
- B. Incident response plan
- C. Disaster recovery plan (DRP)
- D. Business continuity plan (BCP)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 426

An organization recently outsourced the development of a mission-critical business application. Which of the following would be the BEST way to test for the existence of backdoors?

- A. Scan the entire application using a vulnerability scanning tool.
- B. Run the application from a high-privileged account on a test system.
- C. Perform security code reviews on the entire application.
- D. Monitor Internet traffic for sensitive information leakage.

Answer: ([SHOW ANSWER](#))

The best way to test for the existence of backdoors in a mission-critical business application that was outsourced to a third-party developer is to perform security code reviews on the entire application. A backdoor is a hidden or undocumented feature or function in a software application that allows unauthorized or remote access, control, or manipulation of the application or the system it runs on. Backdoors can be intentionally or unintentionally introduced by the developers,

or maliciously inserted by the attackers, and they can pose serious security risks and threats to the organization and its data. Security code reviews are the process of examining and analyzing the source code of a software application to identify and eliminate any security vulnerabilities, flaws, or weaknesses, such as backdoors, that may compromise the functionality, performance, or integrity of the application or the system. Security code reviews can be performed manually by the security experts, or automatically by the security tools, or both, and they can be done at different stages of the software development life cycle, such as design, coding, testing, or deployment. Security code reviews can help to detect and remove any backdoors in the application before they can be exploited by the attackers, and they can also help to improve the quality, reliability, and security of the application.

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 87, page 812; CISM ITEM DEVELOPMENT GUIDE, page 63.

NEW QUESTION: 427

An information security manager learns that IT personnel are not adhering to the information security policy because it creates process inefficiencies. What should the information security manager do FIRST?

- A.** Conduct user awareness training within the IT function.
- B.** Propose that IT update information security policies and procedures.
- C.** Determine the risk related to noncompliance with the policy.
- D.** Request that internal audit conduct a review of the policy development process,

Answer: (SHOW ANSWER)

The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

NEW QUESTION: 428

Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?

- A.** Perform a vulnerability assessment
- B.** Perform a gap analysis to determine needed resources

- C. Create a security exception
- D. Assess the risk to business operations

Answer: ([SHOW ANSWER](#))

According to the CISM Manual, the information security manager should first assess the risk to business operations before taking any other action. This will help to prioritize the issues and determine the appropriate response. Performing a vulnerability assessment, a gap analysis, or creating a security exception are possible actions, but they should be based on the risk assessment results. References = CISM Manual, 5th Edition, page 1211; CISM Practice Quiz, question 32

NEW QUESTION: 429

Which of the following BEST indicates ongoing senior management commitment to the organization's information security strategy?

- 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: D ([LEAVE A REPLY](#))

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: 430

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

- A. Legal
- B. Information security
- C. Help desk
- D. Human resources (HR)

Answer: ([SHOW ANSWER](#))

Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner." SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process." IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access." Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets. HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

NEW QUESTION: 431

Which of the following presents the GREATEST challenge to a large multinational organization using an automated identity and access management (IAM) system?

- A. Large number of applications in the organization
- B. Frequent changes to user roles during employment
- C. Staff turnover rates that significantly exceed industry averages
- D. Inaccurate workforce data from human resources (HR)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 432

A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?

- A. Mitigate
- B. Accept
- C. Transfer
- D. Avoid

Answer: ([SHOW ANSWER](#))

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures.

A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched.

Therefore, mitigate is the correct answer.

References:

<https://simplicable.com/risk/risk-treatment>

<https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/>

<https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment>.

NEW QUESTION: 433

Which of the following would be MOST useful when determining the business continuity strategy for a large organization's data center?

- A. Stakeholder feedback analysis
- B. Business continuity risk analysis
- C. Incident root cause analysis
- D. Business impact analysis (BIA)

Answer: ([SHOW ANSWER](#))

According to the CISM Review Manual, a business impact analysis (BIA) is the most useful tool when determining the business continuity strategy for a large organization's data center, as it helps to identify and prioritize the critical business processes and resources that depend on the data center, and the impact of their disruption or loss. A BIA also provides the basis for defining the recovery time objectives (RTOs) and recovery point objectives (RPOs) for the data center, which guide the selection of the appropriate business continuity strategy.

References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.5.2, page 1511.

NEW QUESTION: 434

When assigning a risk owner, the MOST important consideration is to ensure the owner has:

- A. adequate knowledge of risk treatment and related control activities.
- B. decision-making authority and the ability to allocate resources for risk.
- C. sufficient time for monitoring and managing the risk effectively.

D. risk communication and reporting skills to enable decision-making.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation = The risk owner is the person or entity with the accountability and authority to manage a risk. The risk owner should have the decision-making authority and the ability to allocate resources for risk treatment and related control activities. The risk owner should also be responsible for monitoring and reporting on the risk, but these are not the most important considerations when assigning a risk owner. The risk owner may not have adequate knowledge of risk treatment and related control activities, but can delegate or consult with experts as needed. The risk owner should also have sufficient time for managing the risk effectively, but this is not a prerequisite for assigning a risk owner.

References =

* CISM Review Manual 15th Edition, page 76

* CISM Practice Quiz, question 4171

NEW QUESTION: 435

Which of the following BEST indicates that information security governance and corporate governance are integrated?

- A.** The information security team is aware of business goals.
- B.** The board is regularly informed of information security key performance indicators (KPIs),
- C.** The information security steering committee is composed of business leaders.
- D.** A cost-benefit analysis is conducted on all information security initiatives.

Answer: ([SHOW ANSWER](#))

The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management.

The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

NEW QUESTION: 436

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*

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 437

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: 438

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: ([SHOW ANSWER](#))

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: 439

Which of the following is MOST important to the ongoing success of an information security program?

- A. Executive sponsorship
- B. Skilled personnel
- C. Process automation
- D. Regular awareness training

Answer: ([SHOW ANSWER](#))

Executive sponsorship (A) is the most critical factor for the long-term success of an information security program. CISM emphasizes that leadership support enables funding, enforcement, cross-functional cooperation, and cultural adoption. Skilled staff (B), automation (C), and training (D) are important but depend on sustained executive backing to remain effective. Without sponsorship, security initiatives often lack authority and momentum.

References: ISACA CISM Review Manual (Governance-leadership and sponsorship); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 440

Which of the following should be the PRIMARY focus for an information security manager when reviewing access controls for data stored in an off-premise cloud environment?

- A. Reviewing and updating access controls in response to changes in organizational structure
- B. Implementing strong password policies and enforcing regular password changes
- C. Ensuring access is granted to only those individuals whose job functions require it
- D. Implementing strong encryption protocols to protect sensitive data

Answer: (SHOW ANSWER)

The principle of least privilege-ensuring access is granted only to those whose job functions require it-is the primary control for securing data, especially in cloud environments.

"Access to information and systems should be based on the principles of least privilege and need to know, regardless of environment."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Access Control Management ISACA's CISM practice questions consistently highlight this principle as central to effective cloud security.

NEW QUESTION: 441

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: 442

When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

- A. Data is encrypted in transit and at rest at the vendor site.
- B. Data is subject to regular access log review.
- C. The vendor must be able to amend data.
- D. The vendor must agree to the organization's information security policy,

Answer: (SHOW ANSWER)

When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization's information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization's information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization's right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

NEW QUESTION: 443

Prior to implementing a bring your own device (BYOD) program, it is MOST important to:

- A. select mobile device management (MDM) software.
- B. survey employees for requested applications.
- C. develop an acceptable use policy.
- D. review currently utilized applications.

Answer: (SHOW ANSWER)

Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non-compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.

References = CISM Review Manual, 16th Edition, page 197

NEW QUESTION: 444

Which of the following tasks would provide a newly appointed information security manager with the BEST view of the organization's existing security posture?

- A. Reviewing policies and procedures
- B. Performing a risk assessment
- C. Interviewing business managers and employees
- D. Performing a business impact analysis (BIA)

Answer: (SHOW ANSWER)

Performing a risk assessment gives a holistic and objective understanding of the threats, vulnerabilities, and controls across the organization. It reveals actual risk exposures and the effectiveness of current controls, which directly reflect the organization's security posture.

"Risk assessments identify and evaluate risk and provide the basis for determining how those risks should be managed and mitigated."

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

According to ISACA's CISM Practice Question Database, performing a risk assessment is prioritized over reviewing documents or conducting interviews because it offers direct insight into current exposures and control effectiveness.

NEW QUESTION: 445

Which of the following metrics would provide an accurate measure of an information security program's performance?

- A. A collection of quantitative indicators that are compared against industry benchmarks
- B. A collection of qualitative indicators that accurately measure security exceptions
- C. A combination of qualitative and quantitative trends that enable decision making
- D. A single numeric score derived from various measures assigned to the security program

Answer: (SHOW ANSWER)

NEW QUESTION: 446

An organization finds it necessary to quickly shift to a work-fromhome model with an increased need for remote access security.

Which of the following should be given immediate focus?

- A. Moving to a zero trust access model
- B. Enabling network-level authentication
- C. Enhancing cyber response capability

D. Strengthening endpoint security

Answer: ([SHOW ANSWER](#))

Strengthening endpoint security is the most immediate focus when shifting to a work-from-home model with an increased need for remote access security, as this reduces the risk of unauthorized access, data leakage, malware infection, and other threats that may compromise the confidentiality, integrity, and availability of the organization's information assets. Moving to a zero trust access model, enabling network-level authentication, and enhancing cyber response capability are also important, but not as urgent as strengthening endpoint security, as they require more time, resources, and planning to implement effectively. References = CISM Review Manual 2023, page 1561; CISM Review Questions, Answers & Explanations Manual 2023, page 302; ISACA CISM - iSecPrep, page 153

NEW QUESTION: 447

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

- A.** A manual rather than an automated process is used to compare program versions.
- B.** Users are not notified of scheduled system changes.
- C.** The development manager migrates programs into production.
- D.** Fallback processes are tested the weekend before changes are made.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 448

Of the following, who is responsible for ensuring security controls are aligned with business objectives and regulatory requirements?

- A.** Risk owner
- B.** Control owner
- C.** Compliance manager
- D.** Control assessor

Answer: ([SHOW ANSWER](#))

The correct answer is A because the risk owner is accountable for managing risk associated with a business process, asset, or activity. Since risks arise in a business context, the risk owner must ensure that selected controls align with business objectives, risk appetite, and applicable regulatory requirements. Control owners are responsible for implementing, operating, and maintaining specific controls, but they do not own the business risk itself. Compliance managers help interpret and monitor compliance requirements, but they are not usually accountable for business risk treatment decisions. Control assessors evaluate whether controls are designed and operating effectively, but they do not own the risk or determine business alignment. CISM places strong emphasis on business ownership of information risk. Information security managers support and advise, but accountability for risk remains with the business or risk owner. Therefore, the risk owner is responsible for ensuring that controls appropriately support business objectives and regulatory obligations.

Reference: CISM Information Risk Management; risk ownership, accountability, control alignment, and regulatory compliance principles.

NEW QUESTION: 449

The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:

- A. the organization has the required funds to implement the plan.
- B. compliance with legal and regulatory requirements.
- C. staff participation in information security efforts.
- D. the plan aligns with corporate governance.

Answer: (SHOW ANSWER)

The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly¹. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization². The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives³. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation⁴. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253: CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA, 2017, page 27.

Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION: 450

An organization wants to integrate information security into its HR management processes. Which of the following should be the FIRST step?

- 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: 451

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 EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (**1193** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 452

Which of the following activities **MUST** be performed by an information security manager for change requests?

- A. Perform penetration testing on affected systems.
- B. Assess impact on information security risk.
- C. Review change in business requirements for information security.
- D. Scan IT systems for operating system vulnerabilities.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 453

Which of the following **BEST** enables staff acceptance of information security policies?

- A. Strong senior management support
- B. Computer-based training
- C. Arobust incident response program
- D. Adequate security funding

Answer: ([SHOW ANSWER](#))

= 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: 454

Which of the following is the **BEST** reason for an organization to use Disaster Recovery as a Service (DRaaS)?

- A. It lowers the annual cost to the business.
- B. It eliminates the need to maintain offsite facilities.
- C. It eliminates the need for the business to perform testing.
- D. It transfers the risk associated with recovery to a third party.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 455

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: 456

Which of the following should an information security manager do FIRST when a vulnerability has been disclosed?

- A. Perform a patch update.
- B. Conduct a risk assessment.
- C. Perform a penetration test.
- D. Conduct an impact assessment.

Answer: ([SHOW ANSWER](#))

According to the CISM Review Manual, the first step an information security manager should take when a vulnerability has been disclosed is to conduct a risk assessment to determine the likelihood and impact of the vulnerability being exploited, and the appropriate response strategy. Performing a patch update, a penetration test or an impact assessment are possible subsequent steps, but not the first one.

References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.3.2, page 1331.

NEW QUESTION: 457

The results of a risk assessment for a potential network reconfiguration reveal a high likelihood of sensitive data being compromised. What is the information security manager's BEST course of action?

- A. Recommend additional network segmentation.
- B. Seek an independent opinion to confirm the findings.

- C. Determine alignment with existing regulations.
- D. Report findings to key stakeholders.

Answer: ([SHOW ANSWER](#))

The information security manager's best course of action is to report the findings of the risk assessment to the key stakeholders, such as senior management, business owners, and regulators. This will ensure that the stakeholders are aware of the potential impact of the risk and can make informed decisions on how to address it. The other options are possible actions to take after reporting the findings, but they are not the best course of action in this scenario.

References = CISM Domain 2: Information Risk Management (IRM) [2022 update] (section: Information Risk Response) and CISM ITEM DEVELOPMENT GUIDE - ISACA (page 6, item example 2)

NEW QUESTION: 458

Which of the following has the MOST influence on the information security investment process?

- A. Organizational risk appetite
- B. Security key performance indicators (KPIs)
- C. IT governance framework
- D. Information security policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 459

When taking a risk-based approach to vulnerability management, which of the following is MOST important to consider when prioritizing a vulnerability?

- A. The information available about the vulnerability
- B. The sensitivity of the asset and the data it contains
- C. IT resource availability and constraints
- D. Whether patches have been developed and tested

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Step-by-Step Explanation:

Risk-based vulnerability management prioritizes vulnerabilities based on the potential impact on critical assets.

- A). The information available about the vulnerability: While important for assessing risk, it does not directly determine the priority.
- B). The sensitivity of the asset and the data it contains: This is the BEST answer because prioritizing vulnerabilities based on the criticality of the affected assets ensures that high-impact threats are addressed first.
- C). IT resource availability and constraints: These are logistical considerations but should not outweigh risk impact.
- D). Whether patches have been developed and tested: Patches are important for remediation but do not determine prioritization.

Reference: CISM Job Practice Area 2 (Risk Management) emphasizes considering asset criticality when prioritizing vulnerabilities.

NEW QUESTION: 460

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

- A. translates information security policies and standards into business requirements.
- B. realigns information security objectives to organizational strategy,
- C. articulates management's intent and information security directives in clear language.
- D. relates the investment to the organization's strategic plan.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 461

Which of the following would BEST enable the timely execution of an incident response plan?

- A. The introduction of a decision support tool
- B. Definition of trigger events
- C. Clearly defined data classification process
- D. Centralized service desk

Answer: ([SHOW ANSWER](#))

Definition of trigger events is the best way to enable the timely execution of an incident response plan because it helps to specify the conditions or criteria that initiate the incident response process. Trigger events are predefined scenarios or indicators that signal the occurrence or potential occurrence of a security incident, such as a ransomware attack, a data breach, a denial-of-service attack, or an unauthorized access attempt.

Definition of trigger events helps to ensure that the incident response team is alerted and activated as soon as possible, as well as to determine the appropriate level and scope of response based on the severity and impact of the incident. Therefore, definition of trigger events is the correct answer.

References:

- * <https://www.atlassian.com/incident-management/kpis/common-metrics>
- * <https://www.varonis.com/blog/incident-response-plan/>
- * <https://holierthantao.com/2023/05/03/minimizing-disruptions-a-comprehensive-guide-to-incident-response-planning-and-execution/>

NEW QUESTION: 462

A global organization is considering its geopolitical security risks. Which of the following is the information security manager's BEST approach?

- A. Seek advice from environmental and physical security experts
- B. Implement a third-party risk management framework
- C. Implement controls that deny access from specific jurisdictions
- D. Seek advice from enterprise risk and legal experts

Answer: ([SHOW ANSWER](#))

Geopolitical risk involves complex legal, political, and compliance issues. The enterprise risk and legal teams are best positioned to provide guidance on how national laws, sanctions, and regulations impact operations and security strategies.

"In cases of geopolitical or cross-jurisdictional risk, coordination with legal and enterprise risk functions is essential for informed decision-making."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Context* Security and technical controls should follow this strategic evaluation.

NEW QUESTION: 463

Which of the following is the BEST security control to minimize the risk of successful ransomware attacks?

- A. Application deny list
- B. Web security gateway
- C. Host intrusion detection system
- D. Application allow list

Answer: ([SHOW ANSWER](#))

The correct answer is D because application allow listing is one of the most effective preventive controls against ransomware execution. Allow listing permits only approved and authorized applications, scripts, or executables to run, thereby reducing the likelihood that malicious ransomware code can execute on endpoints or servers. An application deny list blocks known malicious applications, but it is less effective because attackers can modify filenames, hashes, or code to bypass known deny rules. A web security gateway can help reduce exposure to malicious downloads, phishing links, and compromised websites, but it does not fully prevent ransomware introduced through other channels. A host intrusion detection system may detect suspicious activity, but detection is reactive and may occur after ransomware has already started execution or encryption. CISM risk management principles favor preventive controls where feasible, especially for high-impact threats. Since ransomware success often depends on unauthorized code execution, application allow listing provides stronger protection than the other options. Reference: CISM Information Risk Management; malware prevention, ransomware risk, endpoint controls, and preventive security control principles.

NEW QUESTION: 464

Which of the following trends would be of GREATEST concern when reviewing the performance of an organization's intrusion detection systems (IDSs)?

- A. Decrease in false positives
- B. Increase in false positives
- C. Increase in false negatives
- D. Decrease in false negatives

Answer: ([SHOW ANSWER](#))

An increase in false negatives would be of greatest concern when reviewing the performance of an organization's IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore, a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives.

References = CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

NEW QUESTION: 465

Which of the following BEST enables an organization to increase information security control effectiveness?

- A. Reviewing control implementation progress
- B. Establishing risk metrics
- C. Performing criticality analysis of controls on a quarterly basis
- D. Reassigning control ownership for failing areas

Answer: (SHOW ANSWER)

Establishing risk metrics best enables an organization to increase information security control effectiveness because metrics provide measurable insight into whether controls are reducing risk as intended. CISM emphasizes that control effectiveness must be monitored using meaningful measurements aligned with risk appetite, business objectives, and key risk indicators. Reviewing implementation progress only confirms whether controls are being deployed; it does not prove that controls are effective. Performing periodic criticality analysis may help prioritize controls, but it does not continuously measure performance.

Reassigning ownership may be appropriate when accountability problems exist, but it is reactive and limited to failing areas. Risk metrics enable management to detect control weaknesses, track trends, prioritize improvements, and make informed decisions. They also support continuous improvement by showing whether residual risk is moving toward acceptable levels. Therefore, risk metrics are the best mechanism to increase effectiveness because they connect control performance directly to risk reduction and management objectives.

References:

ISACA CISM Review Manual , Information Security Program Development and Management - metrics, monitoring, and control effectiveness ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 466

For an enterprise implementing a bring your own device program, which of the following would provide the BEST security for corporate data residing on unsecured mobile devices?

- A. Acceptable use policy

- B. Containerization solution
- C. Data loss prevention
- D. Device certification process

Answer: B (LEAVE A REPLY)

The correct answer is B because containerization separates corporate data and applications from personal data and applications on a mobile device. In a bring your own device environment, the organization does not fully control the endpoint because it is personally owned and may be used on untrusted networks or with unmanaged applications. A containerization solution helps protect enterprise information by enforcing encryption, access controls, remote wipe, data sharing restrictions, and policy controls within the corporate container. An acceptable use policy is important, but it is administrative and does not technically protect data stored on the device. Data loss prevention can help detect or block unauthorized data movement, but it may not provide the same direct separation and control over mobile data. A device certification process helps assess device suitability, but certification alone does not secure corporate data after deployment. In CISM, controls should be selected based on risk and effectiveness. Containerization is the strongest option for protecting corporate data on unsecured BYOD devices.

Reference: CISM Information Risk Management; mobile device risk, BYOD security, data protection, and compensating control principles.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)

NEW QUESTION: 467

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: 468

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: 469

Which of the following is the MOST important input to the development of an effective information security strategy?

- A. Well-defined security policies and procedures
- B. Risk and business impact assessments
- C. Current and desired state of security
- D. Business processes and requirements

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 470

Business objectives and organizational risk appetite are MOST useful inputs to the development of information security:

- A. strategy.
- B. standards.
- C. key performance indicators (KPIs).
- D. risk assessments.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 471

Which of the following is the BEST method to ensure compliance with password standards?

- A. Implementing password-synchronization software
- B. Using password-cracking software
- C. Automated enforcement of password syntax rules
- D. A user-awareness program

Answer: ([SHOW ANSWER](#))

Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases¹. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.

Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards². Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards³. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for 2020 - Auth0 2: Password synchronization - Wikipedia 3:

NEW QUESTION: 472

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: 473

Which of the following provides the BEST evidence that a newly implemented security awareness program has been effective?

- A.** There has been an increase in the number of phishing attempts reported.
- B.** Senior management supports funding for ongoing awareness training.
- C.** Employees from each department have completed the required training.
- D.** There have been no reported successful phishing attempts since the training started.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 474

The GREATEST benefit of an effective information security awareness program is the organization's ability to:

- A.** Meet compliance requirements
- B.** Reduce security incidents
- C.** Establish accountability
- D.** Develop meaningful metrics

Answer: ([SHOW ANSWER](#))

The greatest benefit of an effective awareness program is the reduction of security incidents (B). CISM stresses that awareness aims to change behavior, which directly lowers the likelihood of incidents such as phishing, data leakage, and policy violations. Compliance (A), accountability (C), and metrics (D) are secondary outcomes. The true measure of success is improved risk posture through fewer and less severe incidents.

References: ISACA CISM Review Manual (Program management-security awareness and behavior); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 475

After a recovery from a successful malware attack, instances of the malware continue to be discovered. Which phase of incident response was not successful?

- A. EradicationB Recovery
- B. Lessons learned review
- C. Incident declaration

Answer: ([SHOW ANSWER](#))

Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.

References:

<https://www.securitymetrics.com/blog/6-phases-incident-response-plan>

<https://www.atlassian.com/incident-management/incident-response>

<https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/>

NEW QUESTION: 476

An organization has identified an increased threat of external brute force attacks in its environment. Which of the following is the MOST effective way to mitigate this risk to the organization's critical systems?

- A. Implement multi-factor authentication.
- B. Increase the frequency of log monitoring and analysis.
- C. Implement a security information and event management system (SIEM),
- D. Increase the sensitivity of intrusion detection systems (IDSs).

Answer: ([SHOW ANSWER](#))

A brute force attack is a type of cyberattack that attempts to gain unauthorized access to an account, file, or other protected information by trying different combinations of usernames and passwords until finding the correct one. Brute force attacks can be very effective if the target system has weak or default passwords, or if the attacker has access to a large number of potential credentials. To mitigate this risk, an organization should implement multi-factor authentication (MFA) for its critical systems. MFA is a security method that requires users to provide more than one piece of evidence to verify their identity before accessing a system or service.

For example, MFA can involve using a password in addition to a code sent to a phone or email, or using a biometric factor such as a fingerprint or face scan. MFA can significantly reduce the impact of brute force attacks by making it harder for attackers to guess or obtain valid credentials, and by increasing the time and effort required for them to compromise the system. 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

NEW QUESTION: 477

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: 478

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: 479

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: 480

An organization requires that business-critical applications be recovered within 30 minutes in the event of a disaster. Which of the following metrics should be defined in the business continuity plan (BCP) to manage this requirement?

- A. Recovery time objective (RTO)
- B. Recovery point objective (RPO)
- C. Maximum tolerable downtime (MTD)

D. Service level agreement (SLA)

Answer: ([SHOW ANSWER](#))

The Recovery Time Objective (RTO) specifies the maximum acceptable downtime before operations must resume. A 30-minute requirement directly defines the RTO for those systems.

"RTO defines the duration within which systems must be restored following an outage to prevent unacceptable business impact."

- CISM Review Manual 15th Edition, Chapter 3: Business Continuity Planning, Section: Continuity Metrics*

NEW QUESTION: 481

The PRIMARY advantage of single sign-on (SSO) is that it will:

- A.** increase efficiency of access management
- B.** increase the security of related applications.
- C.** strengthen user passwords.
- D.** support multiple authentication mechanisms.

Answer: ([SHOW ANSWER](#))

Single sign-on (SSO) is a technology that allows users to access multiple applications or services with one set of credentials, such as a username and password. The primary advantage of SSO is that it increases the efficiency of access management, as it reduces the need for users to remember and enter multiple passwords for different applications or services. SSO also simplifies the user experience, as they can log in once and access multiple resources without having to switch between different windows or tabs. SSO can also improve the security of related applications, as it reduces the risk of password compromise or phishing attacks.

However, SSO does not strengthen user passwords or support multiple authentication mechanisms by itself. It is a complementary technology that enhances the security and convenience of access management. References = CISM Review Manual, 16th Edition, page 991

The primary advantage of single sign-on (SSO) is that it increases the efficiency of access management. With SSO, users only need to remember one set of credentials to access all of their applications, rather than having to remember multiple usernames and passwords for each application. This simplifies the user experience and helps to reduce the amount of time spent managing access to multiple applications. Additionally, SSO can also increase the security of related applications, as users are not sharing the same credentials across multiple applications, and it can also support multiple authentication mechanisms, such as biometric authentication.

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

Special Discount Code: **freecram**)

NEW QUESTION: 482

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: 483

The PRIMARY reason for creating a business case when proposing an information security project is to:

- A. articulate inherent risks.
- B. provide demonstrated return on investment (ROI).
- C. establish the value of the project in relation to business objectives.
- D. gain key business stakeholder engagement.

Answer: (SHOW ANSWER)

The primary reason for creating a business case when proposing an information security project is to establish the value of the project in relation to the business objectives and to justify the investment required. A business case should demonstrate how the project aligns with the organization's strategy, goals, and mission, and how it supports the business processes and functions. A business case should also include the expected benefits, costs, risks, and alternatives of the project, and provide a clear rationale for choosing the preferred option.

References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 484

Which of the following should be the PRIMARY basis for determining the value of assets?

- A. Cost of replacing the assets
- B. Business cost when assets are not available
- C. Original cost of the assets minus depreciation
- D. Total cost of ownership (TCO)

Answer: ([SHOW ANSWER](#))

The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. References = CISM Review Manual 15th Edition, page 64, page 65.

NEW QUESTION: 485

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: 486

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- A. Documentation of control procedures
- B. Standardization of compliance requirements
- C. Automation of controls
- D. Integration of assurance efforts

Answer: ([SHOW ANSWER](#))

= Standardization of compliance requirements is the best approach to reduce unnecessary duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business

partners. Standardization also facilitates the alignment of compliance activities with the organization's risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. References = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

NEW QUESTION: 487

Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

- A. Each process is assigned to a responsible party.
- B. The contact list is regularly updated.
- C. Minimum regulatory requirements are maintained.
- D. Senior management approval has been documented.

Answer: (SHOW ANSWER)

= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability¹²³. References =

* 1: Information Security Incident Response Escalation Guideline², page 4

* 2: A Practical Approach to Incident Management Escalation¹, section "Step 2: Log the escalation and record the related incident problems that occurred"

* 3: Computer Security Incident Handling Guide⁴, page 18

NEW QUESTION: 488

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: C (LEAVE A REPLY)

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: 489

Communicating which of the following would be MOST helpful to gain senior management support for risk treatment options?

- A. Quantitative loss
- B. Industry benchmarks
- C. Threat analysis
- D. Root cause analysis

Answer: (SHOW ANSWER)

communicating the quantitative loss associated with the risk scenarios and the risk treatment options would be the most helpful to gain senior management support, as it helps to demonstrate the value and effectiveness of the risk treatment options in terms of reducing the likelihood and impact of the risk. Quantitative loss also helps to compare the cost and benefit of the risk treatment options and to prioritize the most critical risks.

Industry benchmarks, threat analysis, and root cause analysis may be useful for understanding and assessing the risk, but they do not directly measure the performance of the risk treatment options.

References = Five Key Considerations When Developing Information Security Risk Treatment Plans, CISM Domain 2: Information Risk Management (IRM) [2022 update]

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!

EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here:

<https://www.edudump.com/exams/ISACA/CISM/premium/> (1193 Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)