ISACA.CISM.v2026-02-06.q450

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	450
Version:	v2026-02-06
# of views:	223
# of Questions views:	4500
https://www.freepdfdumps.com/ISACA.CISM.v2026-02-06.q450.html	

NEW QUESTION: 1
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: D (LEAVE A REPLY)
= 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: 2
What is the BEST way to reduce the impact of a successful ransomware attack?
A. Perform frequent backups and store them offline.
B. Purchase or renew cyber insurance policies.
C. Include provisions to pay ransoms ih the information security budget.
D. Monitor the network and provide alerts on intrusions.
Answer: (SHOW ANSWER)
Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself.
Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

NEW QUESTION: 3
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: B (LEAVE A REPLY)
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: 4
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

NEW QUESTION: 5
Which of the following is the MOST effective way to protect the authenticity of data in transit?
A. Digital signature
B. Private key
C. Access controls
D. Public key
Answer: (SHOW ANSWER)
A digital signature validates the authenticity and integrity of a message or document. It ensures that the data was not tampered with and originated from a verified sender.
"Digital signatures provide non-repudiation and confirm both the identity of the sender and the data integrity during transmission."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Cryptographic Controls*

NEW QUESTION: 6
Which of the following is the BEST source of information to support an organization's information security vision and strategy?

A. Governance policies
B. Metrics dashboard
C. Capability maturity model
D. Enterprise information security architecture
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following should an information security manager do NEXT after creating a roadmap to execute the strategy for an information security program?
A. Obtain consensus on the strategy from the executive board.
B. Review alignment with business goals.
C. Define organizational risk tolerance.
D. Develop a project plan to implement the strategy.
Answer: D (LEAVE A REPLY)
The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors.
A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

NEW QUESTION: 8
Which of the following is the MOST important security consideration when planning to use a cloud service provider in a different country?
A. Ability to logically separate client data
B. Ability to meet service level agreements (SLAs)
C. Ability to meet business resiliency requirements
D. Ability to enforce contractual obligations
Answer: D (LEAVE A REPLY)
When dealing with a provider in another country, the most important consideration is the ability to enforce contractual obligations (D). CISM highlights jurisdictional risk, including differences in laws, regulations, and legal enforcement mechanisms. Logical separation (A), SLAs (B), and resiliency (C) are important but depend on enforceable contracts to be

meaningful. Without enforceability, the organization may lack effective recourse in the event of security failures or breaches.
References: ISACA CISM Review Manual (Governance-legal, regulatory, and third-party risk); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 9
The PRIMARY purpose of vulnerability identification is to:
A. Remediate vulnerabilities before they are exploited
B. Discover control deficiencies
C. Provide vulnerability identifiers for risk reporting
D. Prioritize vulnerability remediation
Answer: A (LEAVE A REPLY)
The primary purpose of identifying vulnerabilities is to remediate them before they can be exploited by malicious actors. While risk reporting and prioritization are part of the overall process, the most immediate goal is remediation.
"Vulnerability assessments identify weaknesses that need to be addressed to reduce risk to acceptable levels and prevent potential exploits."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis This aligns with ISACA's official practice questions, where vulnerability identification directly aims to prevent exploitation.

NEW QUESTION: 10
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: B (LEAVE A REPLY)
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: 11

A department has reported that a security control is no longer effective. Which of the following is the information security manager's BEST course of action?
A. Replace the control
B. Check for defense in depth
C. Assess the control state
D. Report the failure to management
Answer: C (LEAVE A REPLY)
The best first step is to assess the control state to determine why it is ineffective and whether adjustments, replacements, or compensating controls are needed.
"Regularly assess the effectiveness of security controls to ensure they are providing the intended level of protection."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Control Monitoring and Assessment* ISACA practice questions stress that assessing the control state comes before taking further action.

NEW QUESTION: 12
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: A (LEAVE A REPLY)
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: 13
An employee of an organization has reported losing a smartphone that contains sensitive information The BEST step to address this situation is to:
A. disable the user's access to corporate resources.
B. terminate the device connectivity.
C. remotely wipe the device
D. escalate to the user's management
Answer: C (LEAVE A REPLY)
The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user' s management, may not be effective or timely enough to secure the sensitive information on the device.
References:
https://www.security.org/resources/protect-data-lost-device/
https://support.google.com/android/answer/6160491?hl=en
https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

NEW QUESTION: 14
Which of the following business units should own the data that populates an identity management system?
A. Legal
B. Information security
C. Information technology
D. Human resources (HR)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
Which of the following is MOST important for the effective implementation of an information security governance program?
A. Employees receive customized information security training
B. The program budget is approved and monitored by senior management
C. The program goals are communicated and understood by the organization.

D. Information security roles and responsibilities are documented.

Answer: C (LEAVE A REPLY)

The program goals are communicated and understood by the organization is the most important factor for the effective implementation of an information security governance program because it ensures that the program is aligned with the business objectives and supported by the stakeholders. Employees receive customized information security training is not the most important factor, but rather a means to achieve the program goals and raise awareness among the staff. The program budget is approved and monitored by senior management is not the most important factor, but rather a resource to enable the program activities and measure its performance. Information security roles and responsibilities are documented is not the most important factor, but rather a way to define and assign the program tasks and accountabilities. References: https://www.isaca. org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-information-security- governance https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

NEW QUESTION: 16

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: B (LEAVE A REPLY)

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: 17
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. Perform a gap analysis.
B. Implement a program of work to comply with the new legislation.
C. Consult with senior management on the best course of action.
D. Understand the cost of noncompliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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: C (LEAVE A REPLY)
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: 19
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: D (LEAVE A REPLY)
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: 20
Which of the following BEST enables an organization to determine the costs of downtime for a critical application?
A. Fault tree analysis
B. Cost-benefit analysis
C. Return on investment (ROI) analysis
D. Business impact analysis (BIA)
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Determining downtime costs requires understanding the financial and operational impact on the business.
A). Fault tree analysis: Primarily used for identifying the root causes of failures, not for assessing downtime costs.
B). Cost-benefit analysis: Compares the costs and benefits of implementing controls but does not specifically address downtime.
C). Return on investment (ROI) analysis: Evaluates the financial return of an investment rather than the cost of an outage.
D). Business impact analysis (BIA): This is the BEST answer because a BIA identifies the effects of a disruption on critical business functions and quantifies the financial impact, including downtime costs.
Reference: CISM Job Practice Area 3 (Information Security Program Development and Management) discusses BIA as a key component in understanding the financial implications of downtime.

NEW QUESTION: 21
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: B (LEAVE A REPLY)
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: 22
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: 23
Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?
A. It transfers the risk associated with recovery to a third party.
B. It lowers the annual cost to the business.
C. It eliminates the need for the business to perform testing.
D. It eliminates the need to maintain offsite facilities.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?
A. Residual risk
B. Regulatory requirements
C. Risk tolerance
D. Control objectives
Answer: C (LEAVE A REPLY)
The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are

also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance.
References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 25
Data classification is PRIMARILY the responsibility of:
A. the data owner.
B. the data custodian.
C. senior management.
D. the security manager.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following should be implemented to BEST reduce the likelihood of a security breach?
A. A configuration management program
B. An incident response program
C. A data forensics program
D. A layered security program
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders
Answer: D (LEAVE A REPLY)
= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them.
By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION: 28
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. Isolate affected systems to prevent further damage
C. Restore affected systems for normal operations.
D. Estimate the amount of damage caused by the incident.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
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: D (LEAVE A REPLY)
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: 30
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: D (LEAVE A REPLY)
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: 31
Following a successful attack, an information security manager should be confident the malware @ continued to spread at the completion of which incident response phase?
A. Containment
B. Recovery
C. Eradication
D. Identification
Answer: A (LEAVE A REPLY)
According to the CISM Review Manual (Digital Version), page 212, the incident response process consists of six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Containment is the phase where the incident response team isolates the affected systems or networks to prevent further damage or spread of the malware. Eradication is the phase where the incident response team removes the malware and any traces of its activity from the affected systems or networks. Recovery is the phase where the incident response team restores the normal operations of the systems or networks. Identification is the phase where the incident response team detects and analyzes the signs of the incident. Therefore, the information security manager should be

confident that the malware has not continued to spread at the completion of the containment phase, which is the earliest phase where the incident response team can stop the propagation of the malware. References = 1: CISM Review Manual (Digital Version), page 212

NEW QUESTION: 32
Which of the following is an information security manager's MOST important course of action after receiving information about a new cybersecurity threat?
A. Update correlation rules for log monitoring to detect the possible emerging threat.
B. Assess the impact of the new threat on the organization in the event of materialization.
C. Review the enterprise architecture (EA) for vulnerabilities exploited by the threat.
D. Report the threat to senior management immediately to enable an informed decision.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
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: 34
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: C (LEAVE A REPLY)
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: 35
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: D (LEAVE A REPLY)
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: 36
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: 37
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: D (LEAVE A REPLY)
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: 38
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: A (LEAVE A REPLY)
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]

NEW QUESTION: 39
Which of the following is the BEST course of action when an online company discovers a network attack in progress?
A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events
D. Shut off all network access points
Answer: B (LEAVE A REPLY)
The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

NEW QUESTION: 40
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: A (LEAVE A REPLY)
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: 41
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: 42
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: D (LEAVE A REPLY)
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

NEW QUESTION: 43
Which of the following incident response phases involves actions to help safeguard critical systems while maintaining business operations?
A. Recovery
B. Identification
C. Preparation
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which of the following would be the GREATEST obstacle to implementing incident notification and escalation processes in an organization with high turnover?
A. Lack of knowledgeable personnel
B. Lack of alignment with organizational goals
C. Lack of communication processes
D. Lack of process documentation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
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 a risk assessment is performed to evaluate the findings
B. Request funding needed to resolve the top vulnerabilities
C. Report findings to senior management
D. Ensure vulnerabilities found are resolved within acceptable timeframes
Answer: (SHOW ANSWER)

NEW QUESTION: 46
An organization has identified a weakness in the ability of its employees to identify and report cybersecurity incidents. Although training materials have been provided, employees show a lack of interest. Which of the following is the information security manager's BEST course of action?
A. Block network access until security awareness training is complete.
B. Conduct an enterprise cybersecurity risk assessment.
C. Obtain key stakeholder and leadership support.
D. Send an email mandating training for the employees.
Answer: (SHOW ANSWER)
Leadership support reinforces the importance of security awareness and motivates employees to engage with training.
"Security awareness programs are most effective when they have visible support from senior management, reinforcing their importance."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training*

NEW QUESTION: 47
Which of the following is the MOST important constraint to be considered when developing an information security strategy?
A. Legal and regulatory requirements
B. Established security policies and standards
C. Compliance with an international security standard
D. Information security architecture
Answer: A (LEAVE A REPLY)

Legal and regulatory requirements are the most important constraint to be considered when developing an information security strategy, as they define the minimum level of security that the organization must comply with to avoid legal sanctions, fines, or reputational damage. Legal and regulatory requirements may vary depending on the jurisdiction, industry, and type of data that the organization handles, and they may impose specific security controls, standards, or frameworks that the organization must follow.
References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.2.1.11

NEW QUESTION: 48
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: 49
Which of the following control types should be considered FIRST for aligning employee behavior with an organization's information security objectives?
A. Technical security controls
B. Physical security controls
C. Access security controls
D. Administrative security controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?
A. Disaster recovery plan (DRP)
B. Incident response plan

C. Business continuity plan (BCP)
D. Business contingency plan
Answer: C (LEAVE A REPLY)
= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources.
Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:
Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
Restore the essential functions and services as quickly and efficiently as possible.
Protect the health, safety, and welfare of the staff, customers, and partners.
Meet the legal, regulatory, contractual, and ethical obligations of the organization.
Learn from the disaster and improve the business continuity capabilities and readiness of the organization.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

NEW QUESTION: 51
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. Activate the disaster recovery plan (DRP).
B. Invoke the incident response plan.
C. Assess changes in the risk profile.
D. Conduct security awareness training.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
An anomaly-based intrusion detection system (IDS) operates by gathering data on:
A. normal network behavior and using it as a baseline lor 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: A (LEAVE A REPLY)
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: 53
Which of the following is the PRIMARY purpose of an acceptable use policy?
A. To provide steps for carrying out security-related procedures
B. To facilitate enforcement of security process workflows
C. To protect the organization from misuse of information assets
D. To provide minimum security baselines for information assets
Answer: (SHOW ANSWER)
The PRIMARY purpose of an acceptable use policy is to protect the organization from misuse of information assets, such as data, hardware, software, and network resources, by defining the rules and expectations for the authorized and appropriate use of these assets by the users. An acceptable use policy helps to prevent or reduce the risks of security breaches, legal liabilities, reputational damage, or loss of productivity that may result from unauthorized, inappropriate, or unethical use of information assets.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 74: "An acceptable use policy is a policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet." The essentials of an acceptable use policy - Infosec Resources: "An Acceptable Use Policy (henceforward mentioned as "AUP") is agreement between two or more parties to a computer network community, expressing in writing their intent to adhere to certain standards of behaviour with respect to the proper usage of specific hardware & software services." Acceptable use policy template - Workable: "This Acceptable Use Policy sets the minimum requirements for the use of our company's IT resources, including computers, networks, devices, software, and internet. It aims to protect our company and our employees from harm and liability, and to ensure that our IT resources are used appropriately, productively, and securely."

NEW QUESTION: 54
Which of the following risk responses is an example of risk transfer?

A. Utilizing third-party applications
B. Purchasing cybersecurity insurance
C. Moving risk ownership to another department
D. Conducting off-site backups
Answer: (SHOW ANSWER)
Risk transfer involves shifting the impact or financial consequences of a risk to a third party. Purchasing cybersecurity insurance is the most common example, where the organization pays a premium to a provider who assumes certain financial responsibilities in the event of a security incident.
Other options listed do not transfer risk:
A). Using third-party applications may introduce new risks, not transfer existing ones.
C). Moving ownership within the organization is reassignment, not transfer.
D). Off-site backups are a form of risk mitigation, not transfer.
"Risk transfer shifts the financial consequences of a risk to another entity, typically through insurance or contractual arrangements."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* Example: "An organization may transfer the financial impact of a potential data breach through the purchase of cyber insurance."

NEW QUESTION: 55
Which of the following is the BEST approach for addressing noncompliance with security standards?
A. Develop new security standards.
B. Maintain a security exceptions process.
C. Discontinue affected activities until security requirements can be met.
D. Apply additional logging and monitoring to affected assets.
Answer: B (LEAVE A REPLY)
A security exceptions process is the most effective governance mechanism for handling noncompliance with standards because it creates a controlled, risk-based method to manage deviations while maintaining accountability. In CISM terms, standards define minimum acceptable baselines, but real-world constraints (legacy systems, third-party limitations, business urgency) sometimes require temporary or conditional deviations. A formal exception process ensures: the business documents the justification, identifies the risk owner, evaluates risk impact, defines compensating controls, sets an expiration date, and tracks remediation to closure. Creating new standards (A) does not fix noncompliance and can increase confusion.
Stopping activities (C) may be necessary for extreme/unacceptable risk, but it is not the "best approach" in general because it can unnecessarily disrupt business operations. Extra monitoring (D) can be a compensating control, but without a formal exception workflow it lacks governance, approval, and traceability.

References: ISACA CISM Review Manual (Governance-policy/standards, exception handling, risk acceptance and accountability); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 56
Which of the following should be the FIRST consideration when developing a strategy for protecting an organization's data?
A. Access rights
B. Encryption
C. Classification
D. Access monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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: C (LEAVE A REPLY)
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: 58
An organization uses a security standard that has undergone a major revision by the certifying authority. The old version of the standard will no longer be used for organizations wishing to maintain their certifications.
Which of the following should be the FIRST
course of action?
A. Evaluate the cost of maintaining the certification.
B. Review the new standard for applicability to the business.

C. Modify policies to ensure new requirements are covered.
D. Communicate the new standard to senior leadership.
Answer: B (LEAVE A REPLY)
Reviewing the new standard for applicability to the business is the first course of action, as it helps to understand the changes, gaps, and impacts of the revision on the organization's security posture, compliance status, and business objectives. Evaluating the cost of maintaining the certification, modifying policies to ensure new requirements are covered, and communicating the new standard to senior leadership are important steps, but they should be done after reviewing the new standard for applicability to the business. References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.2

NEW QUESTION: 59
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: D (LEAVE A REPLY)
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: 60
An organization engages a third-party vendor to monitor and support a financial application under scrutiny by regulators. Which of the following controls would MOST effectively manage risk to the organization?
A. Disabling vendor access and only re-enabling when access is needed
B. Implementing separation of duties between systems and data
C. Including penalty clauses for noncompliance in the vendor contract
D. Monitoring key risk indicators (KRIs)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

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

NEW QUESTION: 62
Which of the following processes is MOST important for the success of a business continuity plan (BCP)?
A. Scheduling periodic internal and external audits
B. Maintaining copies of the plan at the primary and recovery sites
C. Involving all stakeholders in testing and training
D. Including the board and senior management in plan reviews
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
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: A (LEAVE A REPLY)
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: 64
Which of the following is MOST important to maintain integration among the incident response plan, business continuity plan (BCP). and disaster recovery plan (DRP)?
A. Asset classification
B. Recovery time objectives (RTOs)
C. Chain of custody
D. Escalation procedures
Answer: (SHOW ANSWER)
Recovery time objectives (RTOs) are the maximum acceptable time that an organization can be offline or unavailable after a disruption. RTOs are important to maintain integration among the incident response plan, business continuity plan (BCP), and disaster recovery plan (DRP) because they help align the recovery goals and strategies of each plan. By defining clear and realistic RTOs, an organization can ensure that its IT infrastructure and systems are restored as quickly as possible after a disaster, minimizing the impact on business operations and customer satisfaction.
References = CISM Manual, Chapter 6: Incident Response Planning, Section 6.2: Recovery Time Objectives (RTOs), page 971
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 65
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: 66
An information security team plans to strengthen authentication requirements for a customer-facing site, but there are concerns it will negatively impact the user experience. Which of the following is the information security manager's BEST course of action?
A. Assess business impact against security risk.
B. Quantify the security risk to the business.
C. Refer to industry best practices.
D. Provide security awareness training to customers.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
If the investigation of an incident is not completed within the time allocated in the incident response plan, which of the following actions should be taken by the incident response team?
A. Initiate the escalation process.
B. Continue the investigation.
C. Engage the crisis management team.
D. Invoke the business continuity plan (BCP).
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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: 69
Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?
A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan
Answer: (SHOW ANSWER)
The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type, scope, and complexity of the forensic investigation, the legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The existence of the provider's incident

response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any security incidents that may affect the forensic service or the organization. The existence of the provider's incident response plan can help to protect the confidentiality, integrity, and availability of the forensic evidence or data, as well as to comply with the legal and contractual obligations. However, the existence of the provider's incident response plan does not confirm that the provider has the technical capabilities to execute the forensic service competently and ethically12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance - ISACA2

NEW QUESTION: 70
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?
A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.
Answer: (SHOW ANSWER)
The best course of action when the organization receives complaints from users that some of their files have been encrypted and they are receiving demands for money to decrypt the files is to initiate incident response.
This is because the organization is facing a ransomware attack, which is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and loss to the organization's operations, assets, and reputation. Therefore, the organization needs to quickly activate its incident response plan and team, which are designed to handle such security incidents in a coordinated, effective, and efficient manner. The incident response process involves the following steps1:
Preparation: The incident response team prepares the necessary resources, tools, and procedures to respond to the incident. The team also establishes the roles, responsibilities, and communication channels among the team members and other stakeholders.
Identification: The incident response team identifies the scope, source, and severity of the incident. The team also collects and preserves the relevant evidence and logs for further analysis and investigation.
Containment: The incident response team isolates the affected systems and networks to prevent the spread of the ransomware and limit the impact of the incident. The team also implements temporary or alternative solutions to restore the essential functions and services.

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

NEW QUESTION: 71
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: 72
Which of the following is the BEST way to compete for funding for an information security program in an organization with limited resources?
A. Demonstrate the effectiveness of business continuity plans (BCPs).
B. Report key performance indicator (KPI) trends.
C. Demonstrate that the program enables business activities.
D. Provide evidence of increased security events at peer organizations.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
The goal of securing funding for an information security program often requires aligning the program with business goals and demonstrating its value to the organization. Here's an analysis of each option:
A). Demonstrate the effectiveness of business continuity plans (BCPs): While important, this focuses on continuity rather than the overall value of the information security program to business objectives. This is not the strongest method to justify funding.
B). Report key performance indicator (KPI) trends: KPI trends are useful for tracking performance but may not directly demonstrate how the program supports business activities or adds value.
C). Demonstrate that the program enables business activities: This is the BEST option because it ties the information security program directly to business operations. When

security is seen as an enabler (e.g., reducing risks in critical areas like customer data protection), stakeholders are more likely to allocate resources.
D). Provide evidence of increased security events at peer organizations: This may indicate a general threat landscape but does not provide concrete evidence of the program's value or relevance to the organization's specific goals.
Reference: CISM Job Practice Area 1 (Information Security Governance) emphasizes aligning information security strategies with organizational objectives to gain stakeholder support.

NEW QUESTION: 73
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: A (LEAVE A REPLY)
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: 74
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: D (LEAVE A REPLY)
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: 75
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: (SHOW ANSWER)
During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.
"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

NEW QUESTION: 76
Which of the following is the MOST important reason for an organization to communicate to affected parties that a security incident has occurred?

A. To improve awareness of information security
B. To disclose the root cause of the incident
C. To increase goodwill toward the organization
D. To comply with regulations regarding notification
Answer: D (LEAVE A REPLY)
Complying with regulations regarding notification is the most important reason for an organization to communicate to affected parties that a security incident has occurred, as it helps to avoid legal penalties, fines, or sanctions that may result from failing to notify the relevant authorities, customers, or other stakeholders in a timely and appropriate manner. Additionally, complying with regulations regarding notification may also help to preserve the trust and reputation of the organization, as well as to facilitate the investigation and resolution of the incident.
References = CISM Review Manual 2022, page 3151; CISM Exam Content Outline, Domain 4, Task 4.5

NEW QUESTION: 77
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: 78
Predetermined containment methods to be used in a cybersecurity incident response should be based PRIMARILY on the:
A. number of impacted users.
B. capability of incident handlers.
C. type of confirmed incident.
D. predicted incident duration.
Answer: C (LEAVE A REPLY)
According to the NIST SP 800-61 Computer Security Incident Handling Guide, the type of confirmed incident is one of the most important criteria for choosing a containment strategy, as different types of incidents may require different levels of urgency, scope, and impact1. For example, a denial-of-service attack may require a different containment strategy than a ransomware attack or a data breach.
References = 1: NIST SP 800-61: 3.1. Choosing a Containment Strategy2

NEW QUESTION: 79
Which of the following is the BEST way to address data availability concerns when outsourcing information security administration?
A. Develop service level agreements (SLAs).
B. Require nondisclosure agreements (NDAs).
C. Create contingency plans.
D. Stipulate insurance requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which of the following is the BEST indicator of an organization's information security status?
A. Intrusion detection log analysis
B. Controls audit
C. Threat analysis
D. Penetration test
Answer: B (LEAVE A REPLY)
A controls audit is the best indicator of an organization's information security status, as it provides an independent and objective assessment of the design, implementation, and effectiveness of the information security controls. A controls audit can also identify the strengths and weaknesses of the information security program, as well as the compliance

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

NEW QUESTION: 81
To support effective risk decision making, which of the following is MOST important to have in place?
A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls
Answer: (SHOW ANSWER)
To support effective risk decision making, it is most important to have risk reporting procedures in place.
Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for

effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid- level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION: 82
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: (SHOW ANSWER)
= 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: 83
An information security manager learns that an existing supplier plans to begin using its recently developed generative AI technology for the same scope of service. A risk assessment was performed on the supplier three months ago with no outstanding findings. Which of the following is the BEST course of action to address the associated risk?
A. Suspend the use of the supplier until a risk assessment of the AI technology has been performed
B. Report the change in risk to senior management
C. Review the results of the previous risk assessment
D. Add an indemnity clause in the contractual agreement at the renewal stage
Answer: (SHOW ANSWER)
Generative AI introduces new risks (e.g., data leakage, model poisoning). These risks were not part of the original assessment, so a fresh risk assessment must be conducted before continuing service.
"When a significant change in third-party operations occurs, it necessitates a reassessment of risk before continuing operations."

- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management* This ensures security, compliance, and operational continuity.

NEW QUESTION: 84
Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?
A. Security information and event management (SIEM)
B. Extended detection and response (XDR)
C. Endpoint detection and response (EDR)
D. Network intrusion detection system (NIDS)
Answer: (SHOW ANSWER)
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

NEW QUESTION: 85
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 policy
B. Information security threat profile
C. Information security strategy
D. Information security objectives
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
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: D (LEAVE A REPLY)
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.
Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons

learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.
Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re- evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.
Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.
Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. References = ISACA CISM: PRIMARY goal of a post-incident review should be to?
CISM Exam Overview - Vinsys
CISM Review Manual, Chapter 4, page 176
CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

NEW QUESTION: 87
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: B (LEAVE A REPLY)
= 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: 88
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: 89

Which of the following will BEST enable an effective information asset classification process?

A. Including security requirements in the classification process

B. Analyzing audit findings

C. Reviewing the recovery time objective (RTO) requirements of the asset

D. Assigning ownership

Answer: D (LEAVE A REPLY)

Assigning ownership is the best way to enable an effective information asset classification process, as it establishes the authority and responsibility for the information asset and its protection. The owner of the information asset should be involved in the classification process, as they have the best knowledge of the value, sensitivity, and criticality of the asset, as well as the impact of its loss or compromise. The owner should also ensure that the asset is properly labeled, handled, and secured according to its classification level. (From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Information Asset and Security Classification Procedure1, section 3.1.

NEW QUESTION: 90

An organization is performing due diligence when selecting a third party. Which of the following is MOST helpful to reduce the risk of unauthorized sharing of information during this process?

A. Using secure communication channels

B. Establishing mutual non-disclosure agreements (NDAs)

C. Requiring third-party privacy policies

D. Obtaining industry references

Answer: B (LEAVE A REPLY)

The best option to reduce the risk of unauthorized sharing of information during the due diligence process is B). Establishing mutual non-disclosure agreements (NDAs). This is because NDAs are legal contracts that bind the parties to keep confidential any information that is exchanged or disclosed during the due diligence process. NDAs can help to protect the sensitive data, intellectual property, trade secrets, or business strategies of both the organization and the third party from being leaked, stolen, or misused by unauthorized parties.

NDAs can also specify the terms and conditions for the use, storage, and disposal of the information, as well as the consequences for breaching the agreement.

References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 70, page 18

NEW QUESTION: 91

Which of the following BEST demonstrates that an anti-phishing campaign is effective?

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

NEW QUESTION: 92
Which of the following will BEST facilitate timely and effective incident response?
A. Notifying stakeholders when invoking the incident response plan
B. Assessing the risk of compromised assets
C. Classifying the severity of an incident
D. Including penetration test results in incident response planning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
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: C (LEAVE A REPLY)

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: 94
Which of the following is the PRIMARY reason to conduct a post-incident review?
A. To notify regulatory authorities
B. To determine whether digital evidence is admissible
C. To aid in future risk assessments
D. To improve the response process
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
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: D (LEAVE A REPLY)
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: 96
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: 97
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. Implement a SIEM solution.
B. Establish performance metrics for the team.
C. Perform a post-incident review.
D. Perform a threat analysis.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
The MOST appropriate time to conduct a disaster recovery test would be after:
A. major business processes have been redesigned.
B. the business continuity plan (BCP) has been updated.
C. the security risk profile has been reviewed
D. noncompliance incidents have been filed.
Answer: B (LEAVE A REPLY)
The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well as identify any gaps, issues, or improvement opportunities123. References =
* 1: CISM Review Manual 15th Edition, page 2114
* 2: CISM Practice Quiz, question 1042
* 3: Business Continuity Planning and Disaster Recovery Testing, section "Testing the Plan"

NEW QUESTION: 99
A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?
A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.
D. Initiate the organization's incident response process.
Answer: D (LEAVE A REPLY)
= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability.
The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application. Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action.
Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application. Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual
2023, page 211 1; CISM Practice Quiz 2

NEW QUESTION: 100
When is the BEST time to verify that a production system's security mechanisms meet control objectives?
A. During quality and acceptance checks
B. On a continuous basis through monitoring activities and automated tooling
C. After remediations recommended by penetration tests have been completed

D. During annual internal and compliance audits
Answer: B (LEAVE A REPLY)
While audits and assessments provide periodic insights, the best time to verify that security mechanisms meet control objectives is continuously-through monitoring and automation. Continuous monitoring allows the organization to detect misconfigurations, anomalies, or control failures in real-time, significantly improving response capabilities. Modern environments, especially in production systems, require real-time feedback loops to maintain compliance and effectiveness due to rapidly evolving threats and configuration changes.
"Continuous monitoring provides assurance that controls are operating effectively in real time, enabling timely corrective actions."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Control Monitoring*

NEW QUESTION: 101
When defining a security baseline, it is MOST important that the baseline:
A. can vary depending on the security classification of systems.
B. is uniform for all assets of the same type.
C. is developed based on stakeholder consensus.
D. aligns to key risk indicators (KRIs).
Answer: B (LEAVE A REPLY)
A security baseline is a set of minimum security requirements for a system or asset type. The CISM Review Manual states that a baseline should be uniform for all assets of the same type to ensure consistency, enforceability, and ease of monitoring. This standardization supports effective compliance and security operations. While other factors can influence baseline adjustments, uniformity for similar asset types is most critical.
Reference:ISACA CISM Review Manual, 16th Edition, Page 207, "Establishing Security Baselines".

NEW QUESTION: 102
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: 103
A financial company executive is concerned about recently increasing cyberattacks and needs to take action to reduce risk. The organization would BEST respond by:
A. increasing budget and staffing levels for the incident response team.
B. implementing an intrusion detection system (IDS).
C. revalidating and mitigating risks to an acceptable level.
D. testing the business continuity plan (BCP).
Answer: C (LEAVE A REPLY)
The best response for the organization to reduce risk from increasing cyberattacks is to revalidate and mitigate risks to an acceptable level. This means that the organization should review its current risk profile, identify any new or emerging threats, vulnerabilities, or impacts, and evaluate the effectiveness of its existing controls and countermeasures. Based on this analysis, the organization should implement appropriate risk treatment strategies, such as avoiding, transferring, accepting, or reducing the risks, to achieve its desired risk appetite and tolerance. The organization should also monitor and review the risk situation and the implemented controls on a regular basis, and update its risk management plan accordingly. This approach is consistent with the ISACA Risk IT Framework, which provides guidance on how to align IT risk management with business objectives and value12.
The other options are not the best responses because they are either too narrow or too reactive. Increasing budget and staffing levels for the incident response team may improve the organization's ability to respond to and recover from cyberattacks, but it does not address the root causes or the prevention of the attacks.
Implementing an intrusion detection system (IDS) may enhance the organization's detection and analysis capabilities, but it does not guarantee the protection or mitigation of the attacks. Testing the business continuity plan (BCP) may verify the organization's readiness and resilience to continue its critical operations in the event of a cyberattack, but it does not reduce the likelihood or the impact of the attack. References = Risk IT Framework 1 CISM Review Manual, 16th Edition | Print | English 2, Chapter 3: Information Risk Management, pages 97-
98, 103-104, 107-108, 111-112.

NEW QUESTION: 104
Which of the following is the BEST reason to implement a comprehensive information security management system?
A. To ensure continuous alignment with the organizational strategy
B. To gain senior management support for the information security program
C. To support identification of key risk indicators (KRIs)
D. To facilitate compliance with external regulatory requirements
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition, the primary objective of an information security management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks.
References = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

NEW QUESTION: 105
Which of the following eradication methods is MOST appropriate when responding to an incident resulting in malware on an application server?
A. Disconnect the system from the network.
B. Change passwords on the compromised system.
C. Restore the system from a known good backup.
D. Perform operation system hardening.
Answer: C (LEAVE A REPLY)
Restoring the system from a known good backup is the most appropriate eradication method when responding to an incident resulting in malware on an application server, as it ensures that the system is free of any malicious code and that the data and applications are consistent with the expected state. Disconnecting the system from the network may prevent further spread of the malware, but it does not eradicate it from the system. Changing passwords on the compromised system may reduce the risk of unauthorized access, but it does not remove the malware from the system. Performing operation system hardening may improve the security configuration of the system, but it does not guarantee that the malware is eliminated from the system.
References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.4

NEW QUESTION: 106
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: B (LEAVE A REPLY)
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: 107
Which of the following BEST helps to ensure the effective execution of an organization's disaster recovery plan (DRP)?
A. The plan is reviewed by senior and IT operational management.
B. The plan is based on industry best practices.
C. Process steps are documented by the disaster recovery team.
D. Procedures are available at the primary and failover location.
Answer: D (LEAVE A REPLY)
The best way to ensure the effective execution of a disaster recovery plan (DRP) is to make sure that the procedures are available at both the primary and the failover location, so that the staff can access them in case of a disaster. The procedures should be clear, concise, and updated regularly to reflect the current situation and requirements. Having the procedures available at both locations also helps to avoid confusion and delays in the recovery process.
References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Recovery Plan Development, Page 373.

NEW QUESTION: 108
A new information security manager finds that the organization tends to use short-term solutions to address problems. Resource allocation and spending are not effectively

tracked, and there is no assurance that compliance requirements are being met. What should be done FIRST to reverse this bottom-up approach to security?
A. Create an information security steering committee.
B. Implement an information security awareness training program.
C. Establish an audit committee.
D. Conduct a threat analysis.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Which of the following provides the BEST input to determine the level of protection needed for an IT system?
A. Vulnerability assessment
B. Threat analysis
C. Asset classification
D. Internal audit findings
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
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: A (LEAVE A REPLY)
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: 111
For an e-business that requires high availability, which of the following design principles is BEST?
A. Manual failover to the website of another e-business that meets the user's needs
B. A single point of entry allowing transactions to be received and processed quickly
C. Intelligent middleware to direct transactions from a downed system to an alternative
D. Availability of an adjacent cold site and a standby server with mirrored copies of critical data
Answer: C (LEAVE A REPLY)
Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention.
"Middleware solutions can provide automated failover capabilities, improving system resilience and availability."
- CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section:
Availability and Resilience*
Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

NEW QUESTION: 112
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: D (LEAVE A REPLY)
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: 113
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: D (LEAVE A REPLY)
= 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: 114
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: C (LEAVE A REPLY)
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: 115
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: A (LEAVE A REPLY)
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: 116
An organization has decided to implement an Internet of Things (IoT) solution to remain competitive in the market. Which of the following should information security do FIRST?
A. Recalculate risk profile

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

NEW QUESTION: 117
Which of the following is the PRIMARY reason for executive management to be involved in establishing an enterprise's security management framework?
A. To satisfy auditors' recommendations for enterprise security
B. To determine the desired state of enterprise security
C. To establish the minimum level of controls needed
D. To ensure industry best practices for enterprise security are followed
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which of the following is the BEST way to contain an SQL injection attack that has been detected by a web application firewall?
A. Force password changes on the SQL database.
B. Reconfigure the web application firewall to block the attack.
C. Update the detection patterns on the web application firewall.
D. Block the IPs from where the attack originates.
Answer: B (LEAVE A REPLY)
According to the CISM Review Manual, one of the best ways to contain an SQL injection attack that has been detected by a web application firewall is to reconfigure the web application firewall to block the attack.
This means that the web application firewall should be updated with the latest detection patterns and rules that can identify and prevent SQL injection attacks. By doing so, the web application firewall can reduce the impact and damage of the attack, and prevent further exploitation of the vulnerable database1 The other options are not as effective as reconfiguring the web application firewall to block the attack. Force password changes on the SQL database is a reactive measure that does not address the root cause of the problem, and may cause data loss or corruption if not done properly. Updating the detection patterns on the web application firewall is a preventive measure that can help to detect SQL injection attacks, but it does not stop them from happening in the first place. Blocking IPs from where the attack originates is a defensive measure that can limit or stop

some SQL injection attacks, but it does not protect all possible sources of malicious traffic, and may also affect legitimate users or applications1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 32-33...

NEW QUESTION: 119
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. Security 'strategy
B. Recovery strategy
C. IT strategy
D. Risk mitigation strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 120
An information security manager finds a legacy application has no defined data owner. Of the following, who would be MOST helpful in identifying the appropriate data owner?
A. The individual who has the most privileges within the application
B. The individual who manages the process supported by the application
C. The individual responsible for providing support for the application
D. The individual who manages users of the application
Answer: B (LEAVE A REPLY)
In CISM governance, data ownership is a business accountability, not an IT/technical one. The most helpful person to identify the correct data owner is the individual who manages the business process supported by the application (B), because they are closest to the business purpose, outcomes, and decision- making authority tied to that information. Data owners are typically accountable for data classification, access authorization, acceptable use, retention requirements, and protection needs aligned with business and regulatory obligations. By contrast, the person with the most privileges (A) is often an admin and may only reflect technical access, not accountability. Application support (C) manages operational upkeep, and user management (D) may administer accounts but does not define business responsibility for the information.
Assigning the right owner is critical to enable proper governance controls such as access approvals, risk acceptance, and compliance decisions-especially for legacy systems where responsibilities can drift over time.
References: ISACA CISM Review Manual (Governance-roles and responsibilities, information asset ownership, accountability model); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 121
Which of the following is the BEST method for determining whether new risks exist in legacy systems?
A. Frequent updates to the risk register

B. Frequent security architecture reviews
C. Regularly scheduled security audits
D. Regularly scheduled risk assessments
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
When an organization lacks internal expertise to conduct highly technical forensics investigations, what is the BEST way to ensure effective and timely investigations following an information security incident?
A. Retain a forensics firm prior to experiencing an incident.
B. Provide forensics training to the information security team.
C. Ensure the incident response policy allows hiring a forensics firm.
D. Purchase forensic standard operating procedures.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following change management procedures is MOST likely to cause concern to the information security manager?
A. Fallback processes are tested the weekend before changes are made
B. Users are not notified of scheduled system changes
C. A manual rather than an automated process is used to compare program versions.
D. The development manager migrates programs into production
Answer: D (LEAVE A REPLY)
The change management procedure that is MOST likely to cause concern to the information security manager is the development manager migrating programs into production, because it involves a high-risk activity that could compromise the confidentiality, integrity, and availability of the information systems and data.
Migrating programs into production without proper testing, validation, and approval could introduce errors, vulnerabilities, or conflicts that could affect the performance, functionality, or security of the systems. Fallback processes are tested the weekend before changes are made, users are not notified of scheduled system changes, and a manual rather than an automated process is used to compare program versions are all acceptable change

management procedures that do not pose significant risks to the information security manager. References = CISM Review Manual, 16th Edition, page 3121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1522

NEW QUESTION: 124
Identifying which of the following BEST enables a cyberattack to be contained?
A. The segment targeted by the attack
B. The vulnerability exploited by the attack
C. The threat actor that initiated the attack
D. The IP address of the computer that launched the attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
Which of the following is the MOST important objective when planning an incident response program?
A. Recovering from a disaster
B. Minimizing business impact
C. Ensuring IT resiliency
D. Managing resources
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
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: C (LEAVE A REPLY)
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: 127
Which of the following roles is MOST appropriate to determine access rights for specific users of an application?
A. Data owner
B. Data custodian
C. System administrator

D. Senior management
Answer: (SHOW ANSWER)
The data owner is the most appropriate role to determine access rights for specific users of an application because they have legal rights and complete control over data elements4. They are also responsible for approving data glossaries and definitions, ensuring the accuracy of information, and supervising operations related to data quality5. The data custodian is responsible for the safe custody, transport, and storage of the data and implementation of business rules, but not for determining access rights4. The system administrator is responsible for managing the security and storage infrastructure of data sets according to the organization's data governance policies, but not for determining access rights5. Senior management is responsible for setting the strategic direction and priorities for data governance, but not for determining access rights5.
References: 5 https://www.cpomagazine.com/cyber-security/data-owners-vs-data-stewards-vs-data- custodians-the-3-types-of-data-masters-and-why-you-should-employ-them/ 4 https://cloudgal42.com/data- privacy-difference-between-data-owner-controller-and-data-custodian-processor/

NEW QUESTION: 128
The MOST effective tools for responding to new and advanced attacks are those that detect attacks based on:
A. penetration testing.
B. behavior analysis.
C. signature analysis.
D. data packet analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
An incident response plan is being developed for servers hosting sensitive information. In the event of a breach, who should make the decision to shut down the system?
A. Information security manager
B. Operations manager
C. Incident response team
D. Service owner
Answer: (SHOW ANSWER)

NEW QUESTION: 130
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: B (LEAVE A REPLY)

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: 131

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: A (LEAVE A REPLY)

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: 132
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: B (LEAVE A REPLY)
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: 133
Which of the following is the BEST indication of information security strategy alignment with the "&
A. Percentage of information security incidents resolved within defined service level agreements (SLAs)
B. Percentage of corporate budget allocated to information security initiatives
C. Number of business executives who have attended information security awareness sessions
D. Number of business objectives directly supported by information security initiatives
Answer: (SHOW ANSWER)
The number of business objectives directly supported by information security initiatives is the best indication of information security strategy alignment with the organizational goals and objectives. This metric shows how well the information security strategy is aligned with

the business strategy, and how effectively the information security program is delivering value to the organization. The more business objectives that are supported by information security initiatives, the more aligned the information security strategy is with the organizational goals and objectives.
The other options are not the best indicators of information security strategy alignment, as they do not directly measure the impact or contribution of information security initiatives to the business objectives. The percentage of information security incidents resolved within defined SLAs is a measure of the efficiency and effectiveness of the incident management process, but it does not reflect how well the information security strategy is aligned with the business strategy. The percentage of corporate budget allocated to information security initiatives is a measure of the investment and commitment of the organization to information security, but it does not indicate how well the information security initiatives are aligned with the business objectives or how they are prioritized. The number of business executives who have attended information security awareness sessions is a measure of the awareness and involvement of the senior management in information security, but it does not show how well the information security strategy is aligned with the business strategy or how it supports the business objectives. References = CISM Exam Content Outline | CISM Certification | ISACA, Domain 1, Task 1.1 CISM MASTER CHEAT SHEET - SkillCertPro, Chapter 1, page 2 Certified Information Security Manager (CISM), page 1 Certified Information Security Manager Exam Prep Guide: Aligned with ..., page 1 CISM: Certified Information Security SKILLS COVERED Manager, page 1

NEW QUESTION: 134
Which of the following is the GREATEST value provided by a security information and event management (SIEM) system?
A. Maintaining a repository base of security policies
B. Measuring impact of exploits on business processes
C. Facilitating the monitoring of risk occurrences
D. Redirecting event logs to an alternate location for business continuity plan
Answer: C (LEAVE A REPLY)
A security information and event management (SIEM) system is a tool that collects, analyzes, and correlates security events from various sources, such as firewalls, intrusion detection systems, antivirus software, and other devices. A SIEM system can provide real-time alerts, dashboards, reports, and forensic analysis of security incidents. The greatest value of a SIEM system is that it can facilitate the monitoring of risk occurrences by identifying anomalies, trends, patterns, and indicators of compromise that may otherwise go unnoticed. A SIEM system can also help with incident response, compliance, and audit activities by providing evidence and documentation of security events.
References =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2291

ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2082 The greatest value provided by a Security Information and Event Management (SIEM) system is facilitating the monitoring of risk occurrences. SIEM systems collect, analyze and alert on security-related data from various sources such as firewall logs, intrusion detection/prevention systems, and system logs. This allows organizations to identify security threats in real-time and respond quickly, helping to mitigate potential harm to their systems and data.

NEW QUESTION: 135
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: D (LEAVE A REPLY)
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: 136
When evaluating cloud storage solutions, the FIRST consideration should be:
A. The service level agreement (SLA) for encryption keys
B. Alignment with the organization's data classification policy
C. How the organization's sensitive data will be transferred
D. The volume of data to be stored in the cloud
Answer: B (LEAVE A REPLY)
The first consideration when evaluating cloud storage solutions is alignment with the organization's data classification policy (B). CISM emphasizes that security requirements must be driven by data sensitivity and business value. Before assessing encryption methods, SLAs, or data transfer mechanisms, the organization must determine what type of data will be stored and what protection level is required. Data classification informs confidentiality, integrity, availability, privacy, and regulatory requirements. Evaluating SLAs (A) or transfer methods (C) without understanding data sensitivity risks misalignment with governance and compliance obligations. Data volume (D) is an operational consideration, not a security driver.
References: ISACA CISM Review Manual (Risk management-data classification, cloud risk evaluation); CISM Exam Content Outline (Domain 1).

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

NEW QUESTION: 139
The PRIMARY goal of a post-incident review should be to
A. determine why the incident occurred
B. identify policy changes to prevent a recurrence
C. determine how to improve the incident handling process
D. establish the cost of the incident to the business.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140

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

A. The metric compares the organization's inherent risk against its risk appetite.

B. The metric expresses residual risk relative to risk tolerance.

C. The metric directly maps to an industry risk management framework.

D. The metric is frequently reported to senior management.

Answer: (SHOW ANSWER)

NEW QUESTION: 141

ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?

A. Recommend canceling the outsourcing contract.

B. Request an independent review of the provider's data center.

C. Notify affected customers of the data breach.

D. Determine the extent of the impact to the organization.

Answer: D (LEAVE A REPLY)

The CISO should first determine the extent of the impact to the organization by assessing the nature and scope of the data breach, the type and sensitivity of the data involved, the potential harm to the organization and its customers, and the legal and contractual obligations of the organization and the service provider. This will help the CISO to prioritize the appropriate actions and resources to respond to the incident and mitigate the risks. The other options are possible actions that the CISO may take after determining the impact, depending on the circumstances and the outcomes of the investigation. References = CISM Review Manual 15th Edition, page 2231; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1030

NEW QUESTION: 142

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: B (LEAVE A REPLY)

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: 143
Which of the following is the BEST course of action after management has reviewed an identified risk and determines the risk is below the defined risk appetite?
A. Accept
B. Avoid
C. Transfer
D. Mitigate
Answer: A (LEAVE A REPLY)
When a risk is determined to be below the organization's risk appetite, the most appropriate course of action is to formally accept the risk. Risk acceptance is a valid and cost-effective strategy when the impact and likelihood are within acceptable limits, and the cost of mitigation outweighs the potential loss.
"Risk acceptance is an appropriate response when the level of residual risk is within the organization's defined risk tolerance and appetite."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Avoidance, transfer, or mitigation may be overreactions that waste resources in this context.

NEW QUESTION: 144
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: A (LEAVE A REPLY)

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: 145
Which of the following BEST facilitates the development of a comprehensive information security policy?
A. Alignment with an established information security framework
B. An established internal audit program
C. Security key performance indicators (KPIs)
D. Areview of recent information security incidents
Answer: A (LEAVE A REPLY)
Alignment with an established information security framework is the BEST way to facilitate the development of a comprehensive information security policy, because it provides a consistent and structured approach to define, implement, and maintain the policy across the organization. An information security framework is a set of best practices, standards, and guidelines that help to ensure the effectiveness, efficiency, and compliance of the information security policy.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "An information security framework is a set of best practices, standards, and guidelines that provide a consistent and structured approach to information security governance." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "The information security policy should be aligned with an established information security framework to ensure its effectiveness, efficiency, and compliance."

NEW QUESTION: 146
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?
A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology

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

NEW QUESTION: 147
Which of the following is the GREATEST concern resulting from the lack of severity criteria in incident classification?
A. Statistical reports will be incorrect.
B. The service desk will be staffed incorrectly.
C. Escalation procedures will be ineffective.
D. Timely detection of attacks will be impossible.
Answer: C (LEAVE A REPLY)
The greatest concern resulting from the lack of severity criteria in incident classification is that escalation procedures will be ineffective because they rely on severity criteria to determine when and how to escalate an incident to higher levels of authority or responsibility, and what actions or resources are required for resolving an incident. Statistical reports will be incorrect is not a great concern because they do not affect the incident response process directly, but rather provide information or analysis for improvement or evaluation purposes.
The service desk will be staffed incorrectly is not a great concern because it does not affect the incident response process directly, but rather affects the availability or efficiency of one of its components. Timely detection of attacks will be impossible is not a great concern because it does not depend on severity criteria, but rather on monitoring and alerting mechanisms. 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: 148
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: B (LEAVE A REPLY)
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: 149
Which of the following is the BEST indicator of an emerging incident?
A. A recent security incident at an industry competitor
B. Customer complaints about lack of website availability
C. A weakness identified within an organization's information systems
D. Attempted patching of systems resulting in errors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
Which of the following is the BEST reason for senior management to support a business case for developing a monitoring system for a critical application?
A. An industry peer experienced a recent breach with a similar application.
B. The system can be replicated for additional use cases.
C. The cost of implementing the system is less than the impact of downtime.
D. The solution is within the organization's risk tolerance.
Answer: C (LEAVE A REPLY)
A monitoring system for a critical application can help detect and prevent incidents that could affect the availability, integrity, and confidentiality of the application and its data. The impact of downtime could include loss of revenue, reputation, customer satisfaction, and regulatory compliance. Therefore, the cost of implementing the system should be justified by the potential savings from avoiding or minimizing these impacts.
References = CISM Review Manual, 15th Edition, page 173; An Introduction to Metrics, Monitoring, and Alerting; Business-critical applications: What are they and how do you protect them from cyberattack?

NEW QUESTION: 151
The MOST important information for influencing management's support of information security is:

A. an demonstration of alignment with the business strategy.
B. An identification of the overall threat landscape.
C. A report of a successful attack on a competitor.
D. An identification of organizational risks.
Answer: (SHOW ANSWER)
The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. References: https://www.isaca.org /resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with- business-goals-and-objectives

NEW QUESTION: 152
An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?
A. Wipe and reset the endpoint device.
B. Isolate the endpoint device.
C. Power off the endpoint device.
D. Run a virus scan on the endpoint device.
Answer: B (LEAVE A REPLY)
A compromised endpoint device is a potential threat to the security of the network and the data stored on it.
The best course of action to prevent further damage is to isolate the endpoint device from the network and other devices, so that the attacker cannot access or spread to other

systems. Isolating the endpoint device also allows the information security manager to investigate the incident and determine the root cause, the extent of the compromise, and the appropriate remediation steps. Wiping and resetting the endpoint device may not be feasible or desirable, as it may result in data loss or evidence destruction. Powering off the endpoint device may not stop the attack, as the attacker may have installed persistent malware or backdoors that can resume once the device is powered on again. Running a virus scan on the endpoint device may not be effective, as the attacker may have used sophisticated techniques to evade detection or disable the antivirus software. References = CISM Review Manual, 15th Edition, page 1741; CISM Review Questions, Answers & Explanations Database, question ID 2112; Using EDR to Address Unmanaged Devices - ISACA3; Boosting Cyberresilience for Critical Enterprise IT Systems With COBIT and NIST Cybersecurity Frameworks - ISACA; Endpoint Security: On the Frontline of Cyber Risk.
The best way to reduce the risk associated with a bring your own device (BYOD) program is to implement a mobile device policy and standard. This policy should include guidelines and rules regarding the use of mobile devices, such as acceptable use guidelines and restrictions on the types of data that can be stored or accessed on the device. Additionally, it should also include requirements for secure mobile device practices, such as the use of strong passwords, encryption, and regular patching. A mobile device management (MDM) solution can also be implemented to help ensure mobile devices meet the organizational security requirements. However, it is not enough to simply implement the policy and MDM solution; employees must also be trained on the secure mobile device practices to ensure the policy is followed.

NEW QUESTION: 153
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: 154
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: A (LEAVE A REPLY)
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*

NEW QUESTION: 155
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: A (LEAVE A REPLY)
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: 156

What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?

A. Developing a dashboard for communicating the metrics
B. Agreeing on baseline values for the metrics
C. Benchmarking the expected value of the metrics against industry standards
D. Aligning the metrics with the organizational culture

Answer: D (LEAVE A REPLY)
The most important consideration when establishing metrics for reporting to the information security strategy committee is D. Aligning the metrics with the organizational culture. This is because the metrics should reflect the values, beliefs, and behaviors of the organization and its stakeholders, and support the achievement of the strategic objectives and goals. The metrics should also be relevant, meaningful, and understandable for the intended audience, and provide clear and actionable information for decision making. The metrics should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 5, page 3

NEW QUESTION: 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: (SHOW ANSWER)
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 is MOST helpful in determining an organization's current capacity to mitigate risks?
A. Capability maturity model
B. Vulnerability assessment
C. IT security risk and exposure
D. Business impact analysis (BIA)
Answer: A (LEAVE A REPLY)
A capability maturity model (CMM) is a framework that helps organizations assess and improve their processes and capabilities in various domains, such as software

development, project management, information security, and others1. A CMM defines a set of levels or stages that represent the degree of maturity or effectiveness of an organization's processes and capabilities in a specific domain. Each level has a set of criteria or characteristics that an organization must meet to achieve that level of maturity. A CMM also provides guidance and best practices on how to progress from one level to another, and how to measure and monitor the performance and improvement of the processes and capabilities2.
A CMM is most helpful in determining an organization's current capacity to mitigate risks, because it provides a systematic and objective way to evaluate the strengths and weaknesses of the organization's processes and capabilities related to risk management. A CMM can help an organization identify the gaps and opportunities for improvement in its risk management practices, and prioritize the actions and resources needed to address them. A CMM can also help an organization benchmark its risk management maturity against industry standards or best practices, and demonstrate its compliance with regulatory or contractual requirements3.
The other options are not as helpful as a CMM in determining an organization's current capacity to mitigate risks, because they are either more specific, limited, or dependent on a CMM. A vulnerability assessment is a process of identifying and analyzing the vulnerabilities in an organization's systems, networks, or applications, and their potential impact on the organization's assets, operations, or reputation. A vulnerability assessment can help an organization identify the sources and levels of risk, but it does not provide a comprehensive or holistic view of the organization's risk management maturity or effectiveness4. IT security risk and exposure is a measure of the likelihood and impact of a security breach or incident on an organization's IT assets, operations, or reputation. IT security risk and exposure can help an organization quantify and communicate the level of risk, but it does not provide a framework or guidance on how to improve the organization's risk management processes or capabilities5. A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of a disruption or disaster on an organization's critical business functions, processes, or resources. A BIA can help an organization determine the priorities and requirements for business continuity and disaster recovery, but it does not provide a method or standard for assessing or enhancing the organization's risk management maturity or effectiveness. References = 1:
CMMI Institute - What is CMMI? - Capability Maturity Model Integration 2: Capability Maturity Model and Risk Register Integration: The Right ... 3: Performing Risk Assessments of Emerging Technologies - ISACA 4: CISM Review Manual 15th Edition, Chapter 4, Section 4.2 5: CISM Review Manual 15th Edition, Chapter 4, Section 4.3 : CISM Review Manual 15th Edition, Chapter 4, Section 4.4

NEW QUESTION: 159
Which of the following BEST enables an organization to operate smoothly with reduced capacities when service has been disrupted?

A. Crisis management plan
B. Disaster recovery plan (DRP)
C. Incident response plan
D. Business continuity plan (BCP)
Answer: D (LEAVE A REPLY)
A business continuity plan (BCP) is the best option that enables an organization to operate smoothly with reduced capacities when service has been disrupted, as it defines the processes and procedures to maintain or resume critical business functions and minimize the impact of the disruption on the organization's objectives, customers, and stakeholders. A BCP also includes strategies for resource management, communication, recovery, and testing.
References = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans4

NEW QUESTION: 160
Which of the following is MOST helpful in the development of a cost-effective information security strategy that is aligned with business requirements?
A. Benchmarking against industry peers
B. Categorizing information assets
C. Developing policy standards
D. Enforcing data retention
Answer: A (LEAVE A REPLY)

NEW QUESTION: 161
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: 162
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: C (LEAVE A REPLY)
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: 163
Which type of backup BEST enables an organization to recover data after a ransomware attack?
A. Online backup
B. Incremental backup
C. Differential backup
D. Offline backup
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Recovering from ransomware requires backups that are unaffected by the ransomware attack. Here's why offline backups are most effective:
A). Online backup: These are connected to the network and may also be compromised during an attack.

B). Incremental backup: While efficient, incremental backups rely on previous backups and are typically stored online, making them vulnerable to ransomware.
C). Differential backup: Similar to incremental backups, these are not immune if stored online or on compromised systems.
D). Offline backup: This is the BEST choice as offline backups are stored in a location that is not connected to the network, preventing ransomware from encrypting them.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) includes guidance on establishing robust backup strategies for recovery.

NEW QUESTION: 164
Which of the following is an information security manager's MOST important course of action when responding to a major security incident that could disrupt the business?
A. Follow the escalation process.
B. Identify the indicators of compromise.
C. Notify law enforcement.
D. Contact forensic investigators.
Answer: A (LEAVE A REPLY)
When responding to a major security incident that could disrupt the business, the information security manager's most important course of action is to follow the escalation process. The escalation process is a predefined set of steps and procedures that define who should be notified, when, how, and with what information in the event of a security incident. The escalation process helps to ensure that the appropriate stakeholders, such as senior management, business units, legal counsel, public relations, and external parties, are informed and involved in the incident response process. The escalation process also helps to coordinate the actions and decisions of the incident response team and the business continuity team, and to align the incident response objectives with the business priorities and goals. The escalation process should be documented and communicated as part of the incident response plan, and should be reviewed and updated regularly to reflect the changes in the organization's structure, roles, and responsibilities.
References =
* CISM Review Manual 15th Edition, page 1631
* CISM 2020: Incident Management and Response, video 32
* Incident Response Models3

NEW QUESTION: 165
Which of the following is the BEST indication of an effective disaster recovery planning process?
A. Chain of custody is maintained throughout the disaster recovery process.
B. Post-incident reviews are conducted after each event.
C. Recovery time objectives (RTOs) are shorter than recovery point objectives (RPOs).
D. Hot sites are required for any declared disaster.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
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: A (LEAVE A REPLY)
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: 167
The PRIMARY objective of a post-incident review of an information security incident is to:
A. update the risk profile
B. minimize impact
C. prevent recurrence.
D. determine the impact
Answer: C (LEAVE A REPLY)
post-incident review of an information security incident is a process that aims to identify the root causes, contributing factors, and lessons learned from the incident, and to implement corrective and preventive actions to avoid or mitigate similar incidents in the future. The primary objective of a post-incident review is to prevent recurrence, as it helps to improve the security posture, awareness, and resilience of the organization. Preventing recurrence also helps to reduce the impact and cost of future incidents, as well as to enhance the reputation and trust of the organization. Updating the risk profile, minimizing impact, and determining the impact are not the primary objectives of a post-incident review, although

they may be part of its outcomes or outputs. References = CISM Review Manual, 16th Edition, page 1011

NEW QUESTION: 168
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?
A. Internal security audit
B. External security audit
C. Organizational risk appetite
D. Business impact analysis (BIA)
Answer: C (LEAVE A REPLY)
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

NEW QUESTION: 169
Which of the following is an example of a change to the external threat landscape?
A. Industry security standards have been modified.
B. The organization has been purchased by another entity.
C. A commonly used encryption algorithm has been compromised.
D. The information security program has been outsourced.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 170
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: (SHOW ANSWER)
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: 171
What should be the NEXT course of action when an information security manager has identified a department that is repeatedly not following the security policy?
A. Require department users to repeat security awareness training.
B. Perform a vulnerability assessment on the systems within the department.
C. Report the policy violation to senior management.
D. Introduce additional controls to force compliance with policy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?
A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan
Answer: B (LEAVE A REPLY)
The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability.
This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner.

The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

NEW QUESTION: 173
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: 174
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?
A. Configuration management
B. Risk management
C. Access control management
D. Change management
Answer: D (LEAVE A REPLY)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the organization's business strategy and objectives, as well as complying with applicable laws and regulations1.

The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.
The CISM Exam Content Outline also covers the topic of change management in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:
3.2.2 Change Management
3.2.3 Change Control
3.2.4 Change Implementation
3.2.5 Change Monitoring
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 175
A forensic examination of a PC is required, but the PC has been switched off. Which of the following should be done FIRST?
A. Perform a backup of the hard drive using backup utilities.
B. Perform a bit-by-bit backup of the hard disk using a write-blocking device
C. Perform a backup of the computer using the network
D. Reboot the system using third-party forensic software in the CD-ROM drive
Answer: B (LEAVE A REPLY)
Performing a bit-by-bit backup of the hard disk using a write-blocking device is the first step to do when a forensic examination of a PC is required, but the PC has been switched off because it helps to create a forensically sound copy of the original evidence without altering or damaging it. A bit-by-bit backup, also known as a physical or raw image, is a complete copy of every bit on the hard disk, including the unallocated or deleted data. A write-blocking device is a hardware or software tool that prevents any write operations to the hard disk, such as updating timestamps or changing file attributes. Performing a bit-by-bit backup of the hard disk using a write-blocking device ensures the integrity and authenticity of the evidence and allows the forensic analysis to be conducted on the duplicate image rather than the original source. Therefore, performing a bit-by-bit backup of the hard disk using a write-blocking device is the correct answer.
References:
https://en.wikipedia.org/wiki/Computer_forensics
https://resources.infosecinstitute.com/topic/computer-forensics-forensic-analysis-examination-planning/

https://www.computer-forensics-recruiter.com/topics/examination_steps/

NEW QUESTION: 176
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: B (LEAVE A REPLY)
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: 177
An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?
A. Security requirements are included in the vendor contract
B. External security audit results are reviewed.
C. Service level agreements (SLAs) meet operational standards.
D. Business continuity contingency planning is provided
Answer: A (LEAVE A REPLY)
Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.
References:

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

NEW QUESTION: 178
Which of the following is the MOST appropriate risk response when the risk impact has been determined to be immaterial and the likelihood is very low?
A. Accept
B. Avoid
C. Mitigate
D. Transfer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 179
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: A (LEAVE A REPLY)
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: 180
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 lags.
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: 181
Several months after the installation of a new firewall with intrusion prevention features to block malicious activity, a breach was discovered that came in through the firewall shortly after installation. This breach could have been detected earlier by implementing firewall:
A. application awareness
B. packet filtering
C. log monitoring
D. web surfing controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
Which of the following presents the GREATEST challenge to a large multinational organization using an automated identity and access management (1AM) 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: D (LEAVE A REPLY)

NEW QUESTION: 183
Which of the following BEST indicates that information assets are classified accurately?
A. Appropriate prioritization of information risk treatment
B. Increased compliance with information security policy
C. Appropriate assignment of information asset owners
D. An accurate and complete information asset catalog
Answer: A (LEAVE A REPLY)
The best indicator that information assets are classified accurately is appropriate prioritization of information risk treatment. Information asset classification is the process of assigning a level of sensitivity or criticality to information assets based on their value, impact, and legal or regulatory requirements. The purpose of information asset classification is to facilitate the identification and protection of information assets according

to their importance and risk exposure. Therefore, if information assets are classified accurately, the organization can prioritize the information risk treatment activities and allocate the resources accordingly. The other options are not direct indicators of information asset classification accuracy, although they may be influenced by it.
References = CISM Review Manual 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1031

NEW QUESTION: 184
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. Data protection regulations
C. Type and nature of data
D. Business requirements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:
A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.
D. right to audit is included in the service level agreement (SLA).
Answer: D (LEAVE A REPLY)
= To confirm that a third-party provider complies with an organization's information security requirements, it is most important to ensure that the right to audit is included in the service level agreement (SLA), which is a contract that defines the scope, quality, and terms of the services that the third-party provider delivers to the organization. The right to audit is a clause that grants the organization the authority and opportunity to inspect and verify the third-party provider's security policies, procedures, controls, and performance, either by itself or by an independent auditor, at any time during the contract period or after a security incident. The right to audit can help to ensure that the third-party provider adheres to the organization's information security requirements, as well as to the legal and regulatory standards and obligations, and that the organization can monitor and measure the security risks and issues that arise from the outsourcing relationship. The right to audit can also help to identify and address any gaps, weaknesses, or errors that could compromise the security of the information assets and systems that are shared, stored, or processed by the third-party provider, and to provide feedback and recommendations for improvement and optimization of the security posture and performance.
Security metrics, contract clauses, and the information security policy of the third-party provider are all important elements of ensuring the compliance of the third-party provider

with the organization's information security requirements, but they are not the most important ones. Security metrics are quantitative and qualitative measures that indicate the effectiveness and efficiency of the security controls and processes that the third-party provider implements and reports to the organization, such as the number of security incidents, the time to resolve them, the level of customer satisfaction, or the compliance rate. Security metrics can help to evaluate and compare the security performance and outcomes of the third-party provider, as well as to identify and address any deviations or discrepancies from the expected or agreed levels. Contract clauses are legal and contractual terms and conditions that bind the third-party provider to the organization's information security requirements, such as the confidentiality, integrity, and availability of the information assets and systems, the roles and responsibilities of the parties, the liabilities and penalties for breach or violation, or the dispute resolution mechanisms. Contract clauses can help to enforce and protect the organization's information security interests and rights, as well as to prevent or resolve any conflicts or issues that arise from the outsourcing relationship. The information security policy of the third-party provider is a document that defines and communicates the third-party provider's security vision, mission, objectives, and principles, as well as the security roles, responsibilities, and rules that apply to the third-party provider's staff, customers, and partners. The information security policy of the third-party provider can help to ensure that the third-party provider has a clear and consistent security direction and guidance, as well as to align and integrate the third- party provider's security practices and culture with the organization's security expectations and requirements. References = CISM Review Manual 15th Edition, pages 57-581; CISM Practice Quiz, question
1662

NEW QUESTION: 186
The PRIMARY advantage of involving end users in continuity planning is that they:
A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.
Answer: (SHOW ANSWER)
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION: 187
Recovery time objectives (RTOs) are BEST determined by:
A. business managers
B. business continuity officers
C. executive management
D. database administrators (DBAs).
Answer: (SHOW ANSWER)
Business managers are best suited to determine the recovery time objectives (RTOs) for their business processes and functions, as they have the knowledge and authority to assess the impact of downtime and the acceptable level of service continuity. RTOs are the maximum acceptable time that a business process or function can be disrupted before it causes significant harm to the organization's objectives, reputation, or compliance.
References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.2.1.11

NEW QUESTION: 188
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: D (LEAVE A REPLY)
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: 189
Which of the following provides the MOST comprehensive understanding of an organization's information security posture?
A. Security maturity assessment results
B. Threat analysis of the organization's environment
C. Results of vulnerability assessments
D. External penetration test findings
Answer: A (LEAVE A REPLY)

A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture. "Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models* Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

NEW QUESTION: 190
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: B (LEAVE A REPLY)
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: 191
The PRIMARY purpose of implementing information security governance metrics is to:
A. guide security towards the desired state.
B. measure alignment with best practices.
C. assess operational and program metrics.
D. refine control operations.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 192
Which of the following should be the PRIMARY objective when establishing a new information security program?
A. Executing the security strategy
B. Minimizing organizational risk
C. Optimizing resources
D. Facilitating operational security

Answer: A (LEAVE A REPLY)
According to the CISM Review Manual, the primary objective when establishing a new information security program is to execute the security strategy that has been defined and approved by the senior management. The security strategy provides the direction, scope, and goals for the information security program, and aligns with the business objectives and requirements. Minimizing organizational risk, optimizing resources, and facilitating operational security are possible outcomes or benefits of the information security program, but they are not the primary objective.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.1.1, page 1151.

NEW QUESTION: 193
Which of the following should be done FIRST when establishing an information security governance framework?
A. Gain an understanding of the business and cultural attributes.
B. Contract a third party to conduct an independent review of the program.
C. Conduct a cost-benefit analysis of the framework.
D. Evaluate information security tools and skills relevant for the environment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
Management decisions concerning information security investments will be MOST effective when they are based on:
A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,
Answer: C (LEAVE A REPLY)
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION: 195
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: A (LEAVE A REPLY)
The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.
The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non- compliance. However, SLAs do not necessarily address the specific procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties.
Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems.
However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management.
References = 1, 2, 3, 4, 5
https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident-management- part-1 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident- management-part-1

NEW QUESTION: 196
Which of the following should be the PRIMARY goal of information security?
A. Business alignment
B. Data governance
C. Information management

D. Regulatory compliance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 197
Which type of system is MOST effective for monitoring cyber incidents based on impact and tracking them until they are closed?
A. Endpoint detection and response (EDR)
B. Network intrusion detection system (NIDS)
C. Extended detection and response (XDR)
D. Security information and event management (SIEM)
Answer: D (LEAVE A REPLY)
SIEM systems collect and analyze log data from across the organization, allowing for real-time monitoring, incident correlation, and end-to-end tracking of response activities - including severity classification and closure.
"SIEM tools enable centralized management, prioritization, and documentation of incidents, making them essential for impact tracking and incident lifecycle management." - CISM Review Manual 15th Edition, Chapter 4: Incident Management Systems* While EDR and XDR help detect threats, SIEMs offer the full scope for impact-based tracking.

NEW QUESTION: 198
Which of the following roles is BEST able to influence the security culture within an organization?
A. Chief information security officer (CISO)
B. Chief information officer (CIO)
C. Chief executive officer (CEO)
D. Chief operating officer (COO)
Answer: (SHOW ANSWER)
The CEO is the best able to influence the security culture within an organization because the CEO sets the tone and direction for the organization and has the authority and responsibility to ensure that the organization' s objectives are aligned with its strategy. The CEO can also communicate the importance and value of information security to all stakeholders and foster a culture of security awareness and accountability. The CISO, CIO

and COO are important roles in information security management, but they do not have the same level of influence and authority as the CEO. References = CISM Review Manual, 16th Edition, page 221; CISM Exam Content Outline, Domain 1, Task 12 The Chief Information Security Officer (CISO) is responsible for leading and coordinating an organization's information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to information security, the CISO can help to create a security- aware culture within the organization.

NEW QUESTION: 199
A new information security reporting requirement will soon become effective. Which of the following should be the information security manager's FIRST action?
A. Conduct a cost-benefit analysis related to noncompliance with the new requirement.
B. Perform a gap assessment against the new requirement.
C. Investigate to determine whether the new requirement applies to the business.
D. Inform senior management of the new requirement.
Answer: C (LEAVE A REPLY)
Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily.
"The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Compliance*

NEW QUESTION: 200
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: 201
Which of the following roles has the PRIMARY responsibility to ensure the operating effectiveness of IT controls?
A. Risk owner
B. Control tester
C. IT compliance leader
D. Information security manager
Answer: D (LEAVE A REPLY)
According to the CISM Review Manual, 15th Edition1, the information security manager is responsible for ensuring that the information security program supports the organization's objectives and aligns with applicable laws and regulations. The information security manager is also responsible for overseeing the implementation and maintenance of effective IT controls, as well as monitoring and reporting on their performance.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 1, page 10.

NEW QUESTION: 202
Which of the following is MOST useful to an information security manager when determining the need to escalate an incident to senior?
A. Incident management procedures
B. Incident management policy
C. System risk assessment
D. Organizational risk register
Answer: D (LEAVE A REPLY)
The organizational risk register is the most useful for an information security manager when determining the need to escalate an incident to senior management because it contains a list of identified risks to the organization, their likelihood and impact, and their predefined risk thresholds or targets, which can help the information security manager assess the severity and urgency of the incident and decide whether it requires senior management's attention or action. Incident management procedures are not very useful for this purpose because they do not provide any specific criteria or guidance on when to escalate an incident to senior management. Incident management policy is not very useful for this purpose because it does not provide any specific criteria or guidance on when to escalate an incident to senior management. System risk assessment is not very useful for this purpose because it does not reflect the current risk exposure or status of the organization as a whole. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6
/how-to-measure-the-effectiveness-of-information-security-using-iso-27004
https://www.isaca.org/resources
/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned

NEW QUESTION: 203

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: D (LEAVE A REPLY)
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: 204
Which of the following has the GREATEST impact on the effectiveness of an organization's security posture?
A. Incident metrics are frequently compared against industry benchmarks
B. New hires are mandated to attend security training
C. Security is embedded in organizational culture
D. Senior management has approved and endorsed security practices
Answer: C (LEAVE A REPLY)
When security is embedded in organizational culture, it becomes a shared responsibility, increasing adherence and effectiveness.
"A security-aware culture is a key component of an effective security program because it encourages responsible behavior and supports ongoing risk management."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture ISACA's practice questions identify security culture as the foundational element impacting the organization's entire security posture.

NEW QUESTION: 205

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

NEW QUESTION: 206
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: C (LEAVE A REPLY)
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: 207
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: 208

Senior management has just accepted the risk of noncompliance with a new regulation What should the information security manager do NEX*P

A. Report the decision to the compliance officer

B. Update details within the risk register.

C. Reassess the organization's risk tolerance.

D. Assess the impact of the regulation.

Answer: (SHOW ANSWER)

Updating details within the risk register is the next step for the information security manager to do after senior management has accepted the risk of noncompliance with a new regulation because it records and communicates the risk status, impact, and response strategy to the relevant stakeholders. Reporting the decision to the compliance officer is not the next step, but rather a possible subsequent step that involves informing and consulting with the compliance officer about the risk acceptance and its implications. Reassessing the organization's risk tolerance is not the next step, but rather a possible subsequent step that involves reviewing and adjusting the organization's risk appetite and thresholds based on the risk acceptance and its implications. Assessing the impact of the regulation is not the next step, but rather a previous step that involves analyzing and evaluating the potential consequences and likelihood of noncompliance with the regulation. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure- the-effectiveness-of-information-security-using-iso-27004
https://www.isaca.org/resources/isaca-journal

/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

NEW QUESTION: 209
The effectiveness of an information security governance framework will BEST be enhanced if:
A. consultants review the information security governance framework.
B. a culture of legal and regulatory compliance is promoted by management.
C. risk management is built into operational and strategic activities.
D. IS auditors are empowered to evaluate governance activities
Answer: B (LEAVE A REPLY)
The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk management is a key component of information security governance, which 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 and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2:
Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

NEW QUESTION: 210
When integrating security risk management into an organization it is MOST important to ensure:
A. business units approve the risk management methodology.
B. the risk treatment process is defined.
C. information security policies are documented and understood.
D. the risk management methodology follows an established framework.
Answer: A (LEAVE A REPLY)

When integrating security risk management into an organization, it is most important to ensure that the risk management methodology follows an established framework, such as ISO 31000, NIST SP 800-30, or COBIT. This is because a framework provides a consistent and structured approach to identify, assess, treat, and monitor risks, and to align the risk management process with the organization's objectives, culture, and governance. A framework also helps to ensure compliance with relevant standards and regulations, and to facilitate communication and reporting of risks to stakeholders. References: The CISM Review Manual 2023 states that "the risk management methodology should follow an established framework that provides a consistent and structured approach to risk management" and that "the framework should be aligned with the enterprise's objectives, culture, and governance, and should comply with applicable standards and regulations" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "The risk management methodology follows an established framework is the correct answer because it is the most important factor to ensure the successful integration of security risk management into an organization, as it provides a common language and process for managing risks across the organization" (p. 29). Additionally, the article Integrating Risk Management into Business Processes from the ISACA Journal 2018 states that "a risk management framework provides a systematic and comprehensive approach to risk management that covers the entire risk management cycle, from risk identification to risk monitoring and reporting" and that "a risk management framework should be aligned with the organization's strategy, culture, and governance, and should follow recognized standards and best practices, such as ISO 31000, NIST SP 800-30, or COBIT" (p. 1)

NEW QUESTION: 211
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: D (LEAVE A REPLY)
= 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: 212
Who is BEST suited to determine how the information in a database should be classified?
A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner
Answer: D (LEAVE A REPLY)
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements.
Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331

NEW QUESTION: 213
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: 214
An organization learns that a third party has outsourced critical functions to another external provider. Which of the following is the information security manager's MOST important course of action?
A. Engage an independent audit of the third party's external provider.
B. Recommend canceling the contract with the third party.
C. Evaluate the third party's agreements with its external provider.
D. Conduct an external audit of the contracted third party.
Answer: C (LEAVE A REPLY)

According to the CISM Review Manual, the information security manager should evaluate the third party's agreements with its external provider to ensure that the security requirements and controls are adequate and consistent with the organization's expectations. Engaging or conducting an audit may be a subsequent step, but not the most important one. Recommending canceling the contract may be premature and impractical. References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.2, page 1431.

NEW QUESTION: 215
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: 216
The BEST way to integrate information security governance with corporate governance is to ensure:
A. the information security steering committee monitors compliance with security policies.
B. management teams embed information security into business processes.
C. awareness programs include industry best practice for information security governance.
D. the information security program is included in regular external audits.
Answer: B (LEAVE A REPLY)
The best way to integrate information security governance with corporate governance is for management teams to embed information security into business processes. The CISM Review Manual explains that aligning security objectives and activities with organizational

goals and business processes ensures that security is a core part of business operations and strategy, not an isolated activity.
Reference:ISACA CISM Review Manual, 16th Edition, Page 38-39, "Integration of Information Security with Business Processes".

NEW QUESTION: 217
Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?
A. Conducting periodic vulnerability assessments
B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework
Answer: (SHOW ANSWER)
The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

NEW QUESTION: 218
Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?
A. Risk acceptance by the business has been documented
B. Teams and individuals responsible for recovery have been identified
C. Copies of recovery and incident response plans are kept offsite
D. Incident response and recovery plans are documented in simple language
Answer: (SHOW ANSWER)
Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities.
This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

NEW QUESTION: 219
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: C (LEAVE A REPLY)
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: 220
An organization's HR department requires that employee account privileges be removed from all corporate IT systems within three days of termination to comply with a government regulation However, the systems all have different user directories, and it currently takes

up to four weeks to remove the privileges Which of the following would BEST enable regulatory compliance?

A. Multi-factor authentication (MFA) system

B. Identity and access management (IAM) system

C. Privileged access management (PAM) system

D. Governance, risk, and compliance (GRC) system

Answer: B (LEAVE A REPLY)

= An identity and access management (IAM) system is a set of processes, policies, and technologies that enable an organization to manage the identities and access rights of its users across different systems and applications1. An IAM system can help an organization to comply with the government regulation by automating the provisioning and deprovisioning of user accounts, enforcing consistent access policies, and integrating different user directories2. An IAM system can also provide audit trails and reports to demonstrate compliance with the regulation3. A multi-factor authentication (MFA) system is a method of verifying the identity of a user by requiring two or more factors, such as something the user knows, has, or is4. An MFA system can enhance the security of user authentication, but it does not address the issue of removing user privileges from different systems within three days of termination. A privileged access management (PAM) system is a solution that manages and monitors the access of privileged users, such as administrators, to critical systems and resources. A PAM system can reduce the risk of unauthorized or malicious use of privileged accounts, but it does not solve the problem of managing the access of regular users across different systems. A governance, risk, and compliance (GRC) system is a software platform that integrates the functions of governance, risk management, and compliance management. A GRC system can help an organization to align its objectives, policies, and processes with the relevant regulations, standards, and best practices, but it does not directly enable the removal of user privileges from different systems within three days of termination. References = 1: CISM Review Manual (Digital Version), page 24 2: 1 3: 2 4: CISM Review Manual (Digital Version), page 25 : CISM Review Manual (Digital Version), page 26 : CISM Review Manual (Digital Version), page 27

NEW QUESTION: 221

Which of the following is the MOST critical consideration when shifting IT operations to an Infrastructure as a Service (IaaS) model hosted in a foreign country?

A. Labeling of data may help to ensure data is assigned to the correct cloud type.

B. There may be liabilities and penalties in the event of a security breach.

C. Data may be stored in unknown locations and may not be easily retrievable.

D. Laws and regulations of the origin country may not be applicable.

Answer: (SHOW ANSWER)

NEW QUESTION: 222

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: A (LEAVE A REPLY)
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.

NEW QUESTION: 223
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: 224
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: 225
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: D (LEAVE A REPLY)
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: 226
Which of the following is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business?
A. Risk assessment program
B. Information security awareness training
C. Information security governance
D. Information security metrics
Answer: C (LEAVE A REPLY)
= Information security governance is the process of establishing and maintaining the policies, standards, frameworks, and best practices that guide the information security program of an organization. Information security governance helps to ensure that the information security program meets the needs of the business by aligning it with the organization's risk appetite, objectives, and strategy. Information security governance also helps to coordinate and integrate various assurance functions, such as risk management, compliance, audit, and incident response, to provide a holistic view of the information security posture. Information security governance is essential for achieving a positive return on investment (ROI) from information security investments, as well as for enhancing the trust and confidence of internal and external stakeholders. References = CISM Review Manual (Digital Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management1. CISM Review Manual (Print Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management2. CISM ITEM DEVELOPMENT GUIDE, Domain 1: Information Security Governance, Task Statement 1.1, p. 193.
Information security governance is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business. This is because information security governance provides the strategic direction, oversight and accountability for the cybersecurity program. It also ensures that the program aligns with the business objectives, risk appetite and compliance requirements of the organization. Information security governance involves defining roles and responsibilities, establishing policies and standards, setting goals and metrics, allocating resources and monitoring performance of the cybersecurity program.

NEW QUESTION: 227
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: D (LEAVE A REPLY)
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: 228
An employee clicked on a malicious link in an email that resulted in compromising company data. What is the BEST way to mitigate this risk in the future?
A. Conduct phishing awareness training.
B. Implement disciplinary procedures.
C. Establish an acceptable use policy.
D. Assess and update spam filtering rules.
Answer: A (LEAVE A REPLY)
Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

NEW QUESTION: 229
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: 230
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: D (LEAVE A REPLY)
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: 231
Which of the following is MOST important to include in a post-incident review following a data breach?
A. An evaluation of the effectiveness of the information security strategy

B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom
Answer: B (LEAVE A REPLY)
= A post-incident review is a process of analyzing and learning from a security incident, such as a data breach, to improve the security posture and resilience of an organization. A post-incident review should include the following elements12:
* A clear and accurate description of the incident, including its scope, impact, timeline, root cause, and contributing factors.
* A detailed assessment of the effectiveness and efficiency of the incident response process, including the roles and responsibilities, communication channels, coordination mechanisms, escalation procedures, tools and resources, documentation, and reporting.
* An evaluation of the adequacy of existing controls, such as policies, standards, procedures, technical measures, awareness, and training, to prevent, detect, and mitigate similar incidents in the future.
* A list of actionable recommendations and improvement plans, based on the lessons learned and best practices, to address the identified gaps and weaknesses in the security strategy, governance, risk management, and incident management.
* A follow-up and monitoring mechanism to ensure the implementation and verification of the recommendations and improvement plans.
The most important element to include in a post-incident review following a data breach is the evaluation of the adequacy of existing controls, because it directly relates to the security objectives and requirements of the organization, and provides the basis for enhancing the security posture and resilience of the organization.
Evaluating the existing controls helps to identify the vulnerabilities and risks that led to the data breach, and to determine the appropriate corrective and preventive actions to reduce the likelihood and impact of similar incidents in the future. Evaluating the existing controls also helps to align the security strategy and governance with the business goals and objectives, and to ensure the compliance with legal, regulatory, and contractual obligations.
The other elements, such as an evaluation of the effectiveness of the information security strategy, documentation of regulatory reporting requirements, and a review of the forensics chain of custody, are also important, but not as important as the evaluation of the existing controls. An evaluation of the effectiveness of the information security strategy is a broader and more strategic activity that may not be directly relevant to the specific incident, and may require more time and resources to conduct. Documentation of regulatory reporting requirements is a necessary and mandatory task, but it does not provide much insight or value for improving the security posture and resilience of the organization. A review of the forensics chain of custody is a technical and procedural activity that ensures the integrity and admissibility of the digital evidence collected during the incident investigation, but it does not address the root cause or the mitigation of the incident. References = 1: CISM

Exam Content Outline | CISM Certification | ISACA 2: CISM Review Manual 15th Edition, page 147

NEW QUESTION: 232
Which of the following provides the MOST assurance that a third-party hosting provider will be able to meet availability requirements?
A. Right-to-audit clause
B. The third party's incident response plan
C. Service level agreement (SLA)
D. The third party's business continuity plan (BCP)
Answer: C (LEAVE A REPLY)
A Service Level Agreement (SLA) is the contractual document that specifies and guarantees the availability levels the third-party hosting provider must meet. It provides the clearest and most enforceable commitment to availability.
"SLAs establish measurable commitments that can be monitored and enforced, providing a high level of assurance that service availability will meet business requirements."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Outsourcing and Third-Party Management*
ISACA's practice questions highlight SLAs as the most direct and reliable assurance for third-party service availability.

NEW QUESTION: 233
Which of the following BEST determines the data retention strategy and subsequent policy for an organization?
A. Business requirements
B. Risk appetite
C. Supplier requirements
D. Business impact analysis (BIA)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234
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: 235
Which of the following is the BEST way to determine the effectiveness of an incident response plan?
A. Reviewing previous audit reports
B. Conducting a tabletop exercise
C. Benchmarking the plan against best practices
D. Performing a penetration test
Answer: (SHOW ANSWER)
A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

NEW QUESTION: 236
A balanced scorecard MOST effectively enables information security:
A. project management

B. governance.
C. performance.
D. risk management.
Answer: B (LEAVE A REPLY)
A balanced scorecard most effectively enables information security govern-ance.
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 managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress of an organization toward its strategic goals. It typically includes four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:
*Align information security objectives with business objectives and communicate them to senior management and other stakeholders
*Monitor and report on the effectiveness and efficiency of information security processes and controls
*Identify and prioritize improvement opportunities and corrective actions
*Demonstrate the value and benefits of information security investments
*Foster a culture of security awareness and continuous learning
Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality.
A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Per-formance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement.
Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment.
References: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per- formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders:
Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

NEW QUESTION: 237
Which of the following has the MOST influence on the information security investment process?
A. Information security policy
B. Security key performance indicators (KPIs)
C. IT governance framework
D. Organizational risk appetite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 238
Which of the following should have the MOST influence on an organization's response to a new industry regulation?
A. The organization's control objectives
B. The organization's risk management framework
C. The organization's risk appetite
D. The organization's risk control baselines
Answer: C (LEAVE A REPLY)
The most influential factor on an organization's response to a new industry regulation is the organization's risk appetite. This is because the risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives, and it guides the decision-making process for managing risks. The risk appetite also determines the extent to which the organization needs to comply with the new regulation, and the resources and actions required to achieve compliance. The risk appetite should be aligned with the organization's strategy, culture, and values, and it should be communicated and monitored throughout the organization.

NEW QUESTION: 239
During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?
A. Post-incident review
B. Eradication
C. Containment
D. Identification
Answer: (SHOW ANSWER)
The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been

completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2.
The other phases of incident response are:
Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.
Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.
Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2:
What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

NEW QUESTION: 240
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: 241
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. Validate the scope and impact with the business process owner.
B. Initiate the incident response plan.
C. Review and validate the rules within the DLP system.
D. Escalate the issue to senior management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 242
The information security manager of a multinational organization has been asked to consolidate the information security policies of its regional locations. Which of the following would be of GREATEST concern?
A. Varying threat environments
B. Disparate reporting lines
C. Conflicting legal requirements
D. Differences in work culture
Answer: (SHOW ANSWER)
Conflicting legal requirements would be of greatest concern when consolidating the information security policies of regional locations, as they may pose significant challenges and risks for the organization's compliance, privacy, and data protection obligations. Different jurisdictions may have different laws and regulations regarding information security, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.

These laws and regulations may have different definitions, scopes, standards, and enforcement mechanisms for information security, which may create conflicts or inconsistencies when applying a unified policy across the organization.
Therefore, the information security manager should conduct a thorough analysis of the legal requirements of each location, and ensure that the consolidated policy meets the highest level of compliance and avoids any violations or penalties.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task
1.22; CISM 2020: IT Security Policies; Information Security Due Diligence Questionnaire

NEW QUESTION: 243
In the context of developing an information security strategy, which of the following provides the MOST useful input to determine the or
A. Security budget
B. Risk register
C. Risk score
D. Laws and regulations
Answer: D (LEAVE A REPLY)
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with- business-goals-and-objectives

NEW QUESTION: 244
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: A (LEAVE A REPLY)
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: 245
Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?
A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents
Answer: C (LEAVE A REPLY)
Increasing accountability is the primary reason for ensuring clearly defined roles and responsibilities are communicated to users who have been granted administrative privileges due to specific application requirements. Administrative privileges grant users the ability to perform actions that can affect the security, availability and integrity of the application or system, such as installing software, modifying configurations, accessing sensitive data or granting access to other users. Therefore, users who have administrative privileges must be aware of their roles and responsibilities and the consequences of their actions. Communicating clearly defined roles and responsibilities to these users helps to establish accountability by setting expectations, defining boundaries, assigning ownership and enabling monitoring and reporting. Accountability also helps to deter misuse or abuse

of privileges, ensure compliance with policies and standards, and facilitate incident response and investigation.
Clearer segregation of duties is a benefit of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Segregation of duties is a control that aims to prevent or detect conflicts of interest, errors, fraud or unauthorized activities by separating different functions or tasks among different users or groups. For example, a user who can create a purchase order should not be able to approve it. Segregation of duties helps to reduce the risk of unauthorized or inappropriate actions by requiring more than one person to complete a critical or sensitive process. However, segregation of duties alone does not ensure accountability, as users may still act in collusion or circumvent the control.
Increased user productivity is a possible outcome of ensuring clearly defined roles and responsibilities, but it is not the primary reason. User productivity refers to the efficiency and effectiveness of users in performing their tasks and achieving their goals. By communicating clearly defined roles and responsibilities, users may have a better understanding of their tasks, expectations and performance indicators, which may help them to work faster, smarter and better. However, user productivity is not directly related to the security risk of granting administrative privileges, and it may also depend on other factors, such as user skills, motivation, tools and resources.
Fewer security incidents is a desired result of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Security incidents are events or situations that compromise the confidentiality, integrity or availability of information assets or systems. By communicating clearly defined roles and responsibilities, users may be more aware of the security implications of their actions and the potential threats and vulnerabilities they may face, which may help them to avoid or prevent security incidents. However, fewer security incidents is not a guarantee or a measure of accountability, as users may still cause or experience security incidents due to human error, negligence, malicious intent or external factors. References = CISM Review Manual 15th Edition, page 144 Effective User Access Reviews - ISACA1 CISM ITEM DEVELOPMENT GUIDE - ISACA2

NEW QUESTION: 246
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: C (LEAVE A REPLY)
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: 247
Which of the following is MOST important for an information security manager to consider when developing a business continuity plan (BCP) for ransomware attacks?
A. Production data is continuously replicated between primary and secondary sites.
B. Impacted networks can be detached at the network switch level.
C. Backups are maintained offline and regularly tested.
D. Backups are maintained on multiple sites and regularly reviewed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 248
Which of the following MUST happen immediately following the identification of a malware incident?
A. Preparation
B. Recovery
C. Containment
D. Eradication
Answer: (SHOW ANSWER)
Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident12. Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently12. Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization

restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure12. Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware incident12. References = 1: CISM Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA2

NEW QUESTION: 249
Which of the following is the BEST reason to implement an information security architecture?
A. Fast-track the deployment of information security components.
B. Serve as a post-deployment information security road map.
C. Assess the cost-effectiveness of the integration.
D. Facilitate consistent implementation of security requirements.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 250
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?
A. Evaluate the security posture of the organization.
B. Prevent incident recurrence.
C. Identify unmitigated risk.
D. Support business investments in security
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
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: A (LEAVE A REPLY)
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: 252
An organization has multiple data repositories across different departments. The information security manager has been tasked with creating an enterprise strategy for protecting data. Which of the following information security initiatives should be the HIGHEST priority for the organization?
A. Data masking
B. Data retention strategy
C. Data encryption standards
D. Data loss prevention (DLP)
Answer: C (LEAVE A REPLY)
Data encryption standards are the best information security initiative for creating an enterprise strategy for protecting data across multiple data repositories and different departments because they help to ensure the confidentiality, integrity, and availability of data in transit and at rest. Data encryption is a process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt it. Data encryption standards are the rules or specifications that define how data encryption should be performed, such as the type, strength, and mode of encryption, the key management and distribution methods, and the compliance requirements. Data encryption standards help to protect data from unauthorized access, modification, or theft, as well as to meet the regulatory obligations for data privacy and security. Therefore, data encryption standards are the correct answer.
References:
https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data-protection-strategy
https://cloudian.com/guides/data-protection/data-protection-strategy-10-components-of-an-effective-strategy/
https://www.veritas.com/information-center/enterprise-data-protection

NEW QUESTION: 253
A risk owner has accepted a large amount of risk due to the high cost of controls. Which of the following should be the information security manager's PRIMARY focus in this situation?

A. Establishing a strong ongoing risk monitoring process
B. Presenting the risk profile for approval by the risk owner
C. Conducting an independent review of risk responses
D. Updating the information security standards to include the accepted risk
Answer: A (LEAVE A REPLY)
The information security manager's PRIMARY focus in this situation should be establishing a strong ongoing risk monitoring process, which is the process of tracking and evaluating the changes in the risk environment, the effectiveness of the risk responses, and the impact of the residual risk on the organization. A strong ongoing risk monitoring process can help the information security manager to identify any deviations from the expected risk level, to report any significant changes or issues to the risk owner and other stakeholders, and to recommend any adjustments or improvements to the risk management strategy. Presenting the risk profile for approval by the risk owner is not the primary focus in this situation, as it is a step that should be done before the risk owner accepts the risk, not after. Conducting an independent review of risk responses is not the primary focus in this situation, as it is a quality assurance activity that can be performed by an external auditor or a third-party expert, not by the information security manager. Updating the information security standards to include the accepted risk is not the primary focus in this situation, as it is a documentation activity that does not address the ongoing monitoring and reporting of the risk. References = CISM Review Manual, 16th Edition, page 2281; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1022

NEW QUESTION: 254
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: A (LEAVE A REPLY)
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: 255

Which of the following is the MOST important role of the information security manager when the organization is in the process of adopting emerging technologies?
A. Assessing how peer organizations using the same technologies have been impacted
B. Reviewing vendor contracts and service level agreements (SLAs)
C. Developing training for end users to familiarize them with the new technology
D. Understanding the impact on existing resources
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring
Answer: D (LEAVE A REPLY)
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-
1371, page 1, section 1.1.

NEW QUESTION: 257
Which of the following is the MOST effective way to detect information security incidents?
A. Implementation of regular security awareness programs
B. Real-time monitoring of network activity
C. Threshold settings on key risk indicators (KRIs)
D. Periodic analysis of security event log records

Answer: (SHOW ANSWER)

NEW QUESTION: 258
Which of the following is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model?
A. Host patching
B. Penetration testing
C. Infrastructure hardening
D. Data classification
Answer: D (LEAVE A REPLY)
Data classification is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model. Data classification is the process of categorizing data based on its sensitivity, value and criticality to the organization. Data classification helps to determine the appropriate level of protection, access control and retention for different types of data. Data classification is an essential part of data governance and risk management, as it enables the organization to comply with legal and regulatory requirements, protect its intellectual property and reputation, and optimize its data storage and usage costs.
In a SaaS model, the client organization has the least control and responsibility over the cloud infrastructure, platform and application, as these are fully managed by the cloud service provider (CSP). The client organization only has control and responsibility over its own data and users. Therefore, the client organization is responsible for defining and implementing data classification policies and procedures, and ensuring that its data is properly labeled and handled according to its classification level. The client organization is also responsible for educating its users about the importance of data classification and the best practices for data security and privacy.
The other options are not the sole responsibility of the client organization in a SaaS model, as they are either shared with or delegated to the CSP. Host patching, penetration testing and infrastructure hardening are all related to the security and maintenance of the cloud infrastructure and platform, which are the responsibility of the CSP in a SaaS model. The CSP is expected to provide regular updates, patches and fixes to the host operating system, network and application components, and to conduct periodic security assessments and audits to identify and remediate any vulnerabilities or weaknesses in the cloud environment. The client organization may have some responsibility to monitor and verify the CSP's performance and compliance with the service level agreement (SLA) and the cloud security standards and regulations, but it does not have direct control or access to the cloud infrastructure and platform. References = Understanding the Shared Responsibilities Model in Cloud Services - ISACA, Figure 1 CISM Review Manual, Chapter 3, page 121

NEW QUESTION: 259

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. results of exit interviews.

B. previous training sessions.

C. examples of help desk requests.

D. responses to security questionnaires.

Answer: C (LEAVE A REPLY)

The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users' knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:

* Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users' needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.
* Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users' satisfaction, performance, or behavior.
* Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and

appreciate the efforts and contributions of the users and the help desk staff in reporting, responding, or resolving the incidents, and to encourage and motivate them to continue their involvement and participation in information security.
The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information.
Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents that the users may encounter or experience12. References = Information Security Awareness Training: Best Practices
- Infosec Resources, How to Create an Effective Security Awareness Training Program - Infosec Resources, Security Awareness Training: How to Build a Successful Program - ISACA, Security Awareness Training: How to Educate Your Employees - ISACA

NEW QUESTION: 260
From a business perspective, the GREATEST benefit of an incident response plan is that it:
A. Promotes efficiency by providing predefined response procedures
B. Improves security responsiveness to disruptive events
C. Limits the negative impact of disruptive events
D. Ensures compliance with regulatory requirements
Answer: C (LEAVE A REPLY)
The greatest business benefit of an incident response plan is minimizing the negative impact of disruptive incidents on operations and reputation.
"The primary business objective of an incident response plan is to minimize the impact of incidents on business operations and assets."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Objectives* ISACA practice questions reinforce that limiting impact is the key outcome from a business perspective.

NEW QUESTION: 261
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: 262
Which of the following would be MOST useful to help senior management understand the status of information security compliance?
A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Business impact analysis (BIA) results
D. Risk assessment results
Answer: (SHOW ANSWER)
Key performance indicators (KPIs) are measurable values that demonstrate how effectively an organization is achieving its key objectives and goals. KPIs can help senior management understand the status of information security compliance by providing quantifiable and relevant data on the performance and progress of the information security program and processes. KPIs can also help senior management to evaluate the effectiveness and efficiency of the information security controls and activities, identify strengths and weaknesses, and make informed decisions and adjustments. KPIs should be aligned with the organization's strategy, vision, and mission, and should be SMART (specific, measurable, achievable, relevant, and time- bound). Some examples of information security KPIs are: percentage of compliance with policies and standards, number of security incidents and breaches, mean time to detect and respond to incidents, percentage of systems and applications patched, number of security awareness trainings completed, etc.
Industry benchmarks, business impact analysis (BIA) results, and risk assessment results are not the most useful to help senior management understand the status of information security compliance, although they may provide some useful information or insights. Industry benchmarks are comparative measures of the performance or practices of other organizations in the same industry or sector. Industry benchmarks can help senior management to compare and contrast their own information security performance or practices with those of their peers or competitors, and identify gaps or opportunities for improvement. However, industry benchmarks may not reflect the specific goals, needs, or context of the organization, and may not be readily available or reliable. Business impact analysis (BIA) results are the outcomes of the process of analyzing the potential impacts of

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

NEW QUESTION: 263
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: 264
Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?
A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions
C. Effective protection of information assets
D. Optimized allocation of recovery resources
Answer: D (LEAVE A REPLY)
The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

NEW QUESTION: 265
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: B (LEAVE A REPLY)
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: 266
Which of the following is MOST appropriate for an organization to consider when defining incident classification and categorization levels?
A. Maturity of incident response activities
B. Threat environment
C. Quantity of impacted assets
D. Incident impact
Answer: (SHOW ANSWER)
Incident impact is the primary factor for classification and categorization. It ensures incidents are addressed based on their potential to disrupt the organization.
"Incident impact should be the primary factor in defining categorization levels to ensure appropriate prioritization and response."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization* ISACA practice database stresses that focusing on impact ensures incidents receive the proper response priority.

NEW QUESTION: 267
An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?
A. Control owner responses based on a root cause analysis
B. The impact of noncompliance on the organization's risk profile
C. A noncompliance report to initiate remediation activities
D. A business case for transferring the risk
Answer: B (LEAVE A REPLY)
The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions.

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

NEW QUESTION: 268
Which of the following is MOST helpful in determining whether a phishing email is malicious?
A. Reverse engineering
B. Sandboxing
C. Security awareness training
D. Threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 269
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: B (LEAVE A REPLY)
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: 270

The GREATEST challenge when attempting data recovery of a specific file during forensic analysis is when:

A. the partition table on the disk has been deleted.

B. the tile has been overwritten.

C. all files in the directory have been deleted.

D. high-level disk formatting has been performed.

Answer: B (LEAVE A REPLY)

Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.

Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.

However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.4.1.2

NEW QUESTION: 271

Which of the following is the MOST important factor of a successful information security program?

A. The program follows industry best practices.

B. The program is based on a well-developed strategy.

C. The program is cost-efficient and within budget,

D. The program is focused on risk management.

Answer: (SHOW ANSWER)

A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources, implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus. References = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

NEW QUESTION: 272
To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?
A. Gap analysis results
B. Level of residual risk
C. Level of risk treatment
D. Configuration parameters
Answer: B (LEAVE A REPLY)
Level of residual risk is the amount of risk that remains after applying risk treatment options, such as avoidance, mitigation, transfer, or acceptance. The information security manager should compare the level of residual risk with the organization's risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its objectives. The comparison will help to determine whether the risk treatment options are sufficient, excessive, or inadequate, and whether further actions are needed to align the risk level with the risk appetite.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 49: "Residual risk is the risk that remains after risk treatment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 43: "Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value." CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "The information security manager should compare the residual risk with the risk appetite and determine whether the risk treatment options are sufficient, excessive, or inadequate."

NEW QUESTION: 273
A serious vulnerability was detected in a business application that can be exploited by external attackers to compromise the system. What is the information security manager's BEST course of action?
A. Ask the business application owner to apply the fix immediately
B. Implement temporary remediation
C. Immediately shut down the application
D. Report the risk to the business application owner

Answer: B (LEAVE A REPLY)
The best course of action is to implement temporary remediation (B) to reduce exposure while a permanent fix is planned and approved. CISM emphasizes balancing risk reduction with business continuity.
Immediate shutdown (C) or unilateral action (A) may disrupt business operations without proper authorization. Reporting the risk (D) is necessary but insufficient on its own.
Temporary controls, such as access restrictions or additional monitoring, reduce risk while enabling informed decision-making by the business owner.
References: ISACA CISM Review Manual (Program management-risk response and operational controls); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 274
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: C (LEAVE A REPLY)
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: 275
Which of the following is the MOST important reason to involve external forensics experts in evidence collection when responding to a major security breach?
A. To validate the incident response process
B. To provide the response team with expert training on evidence handling
C. To prevent evidence from being disclosed to any internal staff members
D. To ensure evidence is handled by qualified resources
Answer: D (LEAVE A REPLY)

NEW QUESTION: 276
Which of the following BEST illustrates residual risk within an organization?
A. Heat map
B. Business impact analysis (BIA)
C. Risk management framework
D. Balanced scorecard
Answer: A (LEAVE A REPLY)

NEW QUESTION: 277
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: B (LEAVE A REPLY)
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: 278
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?
A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes
Answer: D (LEAVE A REPLY)
Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations. References = CISM Review Manual 2023, page 291; CISM Review Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

NEW QUESTION: 279
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: D (LEAVE A REPLY)
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: 280
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: C (LEAVE A REPLY)
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: 281
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: A (LEAVE A REPLY)
= 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: 282
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. Accept the risk, as the benefits exceed the potential consequences.

B. Mitigate the risk by encrypting the customer names in the data set.
C. Transfer the risk by purchasing insurance.
D. Mitigate the risk by applying anonymization on the data set.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 283
Which of the following is the PRIMARY purpose of a business impact analysis (BIA)?
A. To define security roles and responsibilities
B. To determine return on investment (ROI)
C. To establish incident severity levels
D. To determine the criticality of information assets
Answer: D (LEAVE A REPLY)
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. The primary purpose of a BIA is to determine the criticality of information assets and the impact of their unavailability on the organization's mission, objectives and reputation. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

NEW QUESTION: 284
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: 285
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: 286
To help ensure that an information security training program is MOST effective, its contents should be:
A. based on recent incidents.
B. based on employees' roles.
C. aligned to business processes.
D. focused on information security policy.
Answer: (SHOW ANSWER)
To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles, as different roles have different information security responsibilities, needs, and risks. A role-based training program can tailor the content and delivery methods to suit the specific learning objectives and outcomes for each role, and enhance the relevance and retention of the information security knowledge and skills. Based on recent incidents is not the best answer, as it may not cover all the information security topics that are important for the organization, and may not address the root causes or preventive measures of the incidents. Based on employees' roles is more comprehensive and proactive than based on recent incidents.
Aligned to business processes is not the best answer, as it may not reflect the individual roles and responsibilities of the employees, and may not cover all the information security aspects that are relevant for the organization. Based on employees' roles is more specific and personalized than aligned to business processes. Focused on information security policy is not the best answer, as it may not provide sufficient details or examples to help

the employees understand and apply the information security policy in their daily work. Based on employees' roles is more practical and engaging than focused on information security policy. References = CISM Review Manual, 16th Edition, page 2241; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1002 To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles. This is because different roles have different responsibilities and access levels to information and systems, and therefore face different types of threats and risks. By tailoring the training content to the specific needs and expectations of each role, the training program can increase the relevance and retention of the information security knowledge and skills for the employees. Role-based training can also help employees understand their accountability and obligations for protecting information assets in their daily tasks

NEW QUESTION: 287
Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?
A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.
D. Provide security awareness training to board executives.
Answer: A (LEAVE A REPLY)
The best way to help ensure alignment of the information security program with organizational objectives is A: Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by:
Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators Allocating and prioritizing the resources and budget

for information security initiatives and projects Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

NEW QUESTION: 288
A new type of ransomware has infected an organization's network. Which of the following would have BEST enabled the organization to detect this situation?
A. Monitoring of anomalies in system behavior
B. Periodic information security training for end users
C. Use of integrated patch deployment tools
D. Regular review of the threat landscape
Answer: A (LEAVE A REPLY)

NEW QUESTION: 289
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: 290
Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness program?
A. Percentage of employee computers and devices infected with malware
B. Percentage of employees who regularly attend security training
C. Number of security incidents reported to the help desk

D. Number of phishing emails viewed by end users
Answer: B (LEAVE A REPLY)

NEW QUESTION: 291
Which of the following is the MOST important consideration when defining control objectives?
A. Senior management support
B. Risk appetite
C. Threat environment
D. Budget allocation
Answer: (SHOW ANSWER)
Risk appetite reflects how much risk the organization is willing to tolerate. It is the primary driver when defining control objectives, ensuring alignment with overall business strategy. "Risk appetite should be used to guide the selection and design of control objectives to ensure risk is managed within acceptable boundaries."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management Strategy* Support, budget, and threats matter, but without alignment to risk appetite, controls may be misaligned.

NEW QUESTION: 292
An information security manager has identified that security risks are not being treated in a timely manner.
Which of the following
A. Provide regular updates about the current state of the risks.
B. Re-perform risk analysis at regular intervals.
C. Assign a risk owner to each risk
D. Create mitigating controls to manage the risks.
Answer: B (LEAVE A REPLY)
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: 293
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?
A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.
Answer: C (LEAVE A REPLY)
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

NEW QUESTION: 294
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: D (LEAVE A REPLY)
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: 295
Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?
A. Information security strategy
B. Availability of potential resources
C. Information security incidents
D. Current resourcing levels
Answer: D (LEAVE A REPLY)

NEW QUESTION: 296
When establishing an information security governance framework, it is MOST important for an information security manager to understand:
A. risk management techniques.
B. the threat environment.

C. the corporate culture.
D. information security best practices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
A business impact analysis (BIA) should be periodically executed PRIMARILY to:
A. validate vulnerabilities on environmental changes.
B. analyze the importance of assets.
C. check compliance with regulations.
D. verify the effectiveness of controls.
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12. According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations ©, as these are not the primary purposes of a BIA.
References: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

NEW QUESTION: 298
An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?
A. Enforce the policy.
B. Modify the policy.
C. Present the risk to senior management.
D. Create an exception for the deviation.
Answer: C (LEAVE A REPLY)
The information security manager's best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational

consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role- based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management's approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127-128, 138-139, 143-144.

NEW QUESTION: 299
Which of the following is MOST important when conducting a forensic investigation?
A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody
Answer: D (LEAVE A REPLY)
Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence. References = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

NEW QUESTION: 300
Penetration testing is MOST appropriate when a:
A. new system is about to go live.
B. new system is being designed.
C. security policy is being developed.
D. security incident has occurred,
Answer: A (LEAVE A REPLY)
= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious

source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

NEW QUESTION: 301
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: 302
An organization is transitioning to a Zero Trust architecture. Which of the following is the information security manager's BEST approach for communicating the implications of this transition to the board of directors?
A. Present a diagram of core Zero Trust logical components to help visualize the architectural changes
B. Summarize the training plan and end user feedback in an internal portal and send the link to the board
C. Prepare a report on the Zero Trust implementation that includes a status dashboard and timeline
D. Provide an outline of the business impact in terms of risk reduction and changes in user experience
Answer: D (LEAVE A REPLY)
Senior leadership needs to understand how Zero Trust supports risk reduction and business needs.
Communicating the impact on risk reduction and user experience aligns security initiatives with business goals.
"Communicating how security initiatives support business objectives and risk reduction is critical for gaining senior management support."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment*

NEW QUESTION: 303
Detailed business continuity plans (BCPs) should be PRIMARILY based on:
A. capabilities of available local vendors.
B. cost and resources needed to execute.
C. strategies validated by senior management.
D. strategies that cover all applications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 304
An organization has identified IT failures in a call center application. Of the following, who should own this risk?
A. Head of the call center
B. Information security manager
C. Head of the IT department
D. Chief executive officer (CEO)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
Which of the following is the BEST indication of an effective information security awareness training program?
A. An increase in the frequency of phishing tests
B. An increase in positive user feedback
C. An increase in the speed of incident resolution
D. An increase in the identification rate during phishing simulations
Answer: D (LEAVE A REPLY)
An effective information security awareness training program should aim to improve the knowledge, skills and behavior of the employees regarding information security. One of the ways to measure the effectiveness of such a program is to conduct phishing simulations, which are mock phishing attacks that test the employees' ability to identify and report phishing emails. An increase in the identification rate during phishing simulations indicates that the employees have learned how to recognize and avoid phishing attempts, which is one of the common threats to information security. Therefore, this is the best indication of an effective information security awareness training program among the given options.
The other options are not as reliable or relevant as indicators of an effective information security awareness training program. An increase in the frequency of phishing tests does not necessarily mean that the employees are learning from them or that the tests are aligned with the learning objectives of the program. An increase in positive user feedback may reflect the satisfaction or engagement of the employees with the program, but it does not measure the actual learning outcomes or behavior changes. An increase in the speed of incident resolution may be influenced by other factors, such as the availability and efficiency of the incident response team, the severity and complexity of the incidents, or the tools and processes used for incident management.
Moreover, the speed of incident resolution does not reflect the prevention or reduction of incidents, which is a more desirable goal of an information security awareness training program. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1001.

NEW QUESTION: 306
Which of the following should be the FIRST step in patch management procedures when receiving an emergency security patch?
A. Schedule patching based on the criticality.
B. Install the patch immediately to eliminate the vulnerability.
C. Conduct comprehensive testing of the patch.
D. Validate the authenticity of the patch.
Answer: D (LEAVE A REPLY)
Validating the authenticity of the patch is the first step in patch management procedures when receiving an emergency security patch, as it helps to ensure that the patch is genuine and not malicious. Validating the authenticity of the patch can be done by verifying the source, signature, checksum, or certificate of the patch, and comparing it with the information provided by the software vendor or manufacturer. Installing an unverified patch may introduce malware, compromise the system, or cause unexpected errors or conflicts.
References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.42; Practical Patch Management and Mitigation1; Vulnerability and patch management in the CISSP exam3

NEW QUESTION: 307
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: C (LEAVE A REPLY)
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: 308
What type of control is being implemented when a security information and event management (SIEM) system is installed?
A. Preventive

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

NEW QUESTION: 309
An organization is creating a risk mitigation plan that considers redundant power supplies to reduce the business risk associated with critical system outages. Which type of control is being considered?
A. Preventive
B. Corrective
C. Detective
D. Deterrent
Answer: (SHOW ANSWER)
A preventive control is a type of control that aims to prevent or reduce the occurrence or impact of potential adverse events that can affect the organization's objectives and performance. Preventive controls are proactive measures that are implemented before an incident happens, and they are designed to address the root causes or sources of risk. Preventive controls can also help the organization to comply with the relevant laws, regulations, standards, and best practices regarding information security1.
An example of a preventive control is a redundant power supply, which is a backup or alternative source of power that can be used in case of a power outage or failure. A redundant power supply can reduce the business risk associated with critical system outages, which can result from power disruptions caused by natural disasters, technical faults, human errors, or malicious attacks. A redundant power supply can provide the following benefits for information security2:
* Maintain the availability and continuity of the critical systems and services that depend on power, such as servers, databases, networks, or applications. A redundant power supply

can ensure that the critical systems and services can operate normally or resume quickly after a power outage or failure, minimizing the downtime and data loss that can affect the organization's operations, customers, or reputation.
* Protect the integrity and reliability of the critical systems and data that are stored or processed by the power-dependent devices, such as computers, hard drives, or memory cards. A redundant power supply can prevent or reduce the damage or corruption of the critical systems and data that can be caused by sudden or unexpected power fluctuations, surges, or interruptions, which can compromise the accuracy, completeness, or consistency of the information.
* Enhance the resilience and redundancy of the power infrastructure and network that supports the critical systems and services. A redundant power supply can provide an alternative or backup route for power delivery and distribution, which can increase the flexibility and adaptability of the power infrastructure and network to cope with different scenarios or conditions of power supply or demand.
The other options are not the type of control that is being considered by the organization. A corrective control is a type of control that aims to restore or recover the normal state or function of the affected systems or processes after an incident has occurred. A corrective control is a reactive measure that is implemented during or after an incident, and it is designed to address the consequences or impacts of risk. A corrective control can also help the organization to learn from the incident and improve its information security practices1. An example of a corrective control is a backup or restore system, which is a method of creating and restoring copies of the system or data that have been lost or damaged due to an incident.
A detective control is a type of control that aims to identify or discover the occurrence or existence of an incident or a deviation from the expected or desired state or behavior of the systems or processes. A detective control is a monitoring or auditing measure that is implemented during or after an incident, and it is designed to provide information or evidence of risk. A detective control can also help the organization to analyze or investigate the incident and determine the root cause or source of risk1. An example of a detective control is a log or alert system, which is a tool of recording or reporting the activities or events that have occurred or are occurring within the systems or processes.
A deterrent control is a type of control that aims to discourage or dissuade the potential perpetrators or sources of risk from initiating or continuing an incident or an attack. A deterrent control is a psychological or behavioral measure that is implemented before or during an incident, and it is designed to influence or manipulate the motivation or intention of risk. A deterrent control can also help the organization to reduce the likelihood or frequency of incidents or attacks1. An example of a deterrent control is a warning or notification system, which is a method of communicating or displaying the consequences or penalties of violating the information security policies or rules. References = Risk Control Techniques: Preventive, Corrective, Directive, And ..., Learn Different types of Security Controls in CISSP - Eduonix Blog

NEW QUESTION: 310
Which of the following factors would have the MOST significant impact on an organization's information security governance mode?
A. Outsourced processes
B. Security budget
C. Number of employees
D. Corporate culture
Answer: D (LEAVE A REPLY)
The corporate culture of an organization is the set of values, beliefs, norms, and behaviors that shape how the organization operates and interacts with its stakeholders. The corporate culture can have a significant impact on an organization's information security governance mode, which is the way the organization establishes, implements, monitors, and evaluates its information security policies, standards, and objectives. A strong information security governance mode requires a supportive corporate culture that fosters a shared vision, commitment, and accountability for information security among all levels of the organization. A supportive corporate culture can also help to overcome resistance to change, promote collaboration and communication, encourage innovation and learning, and enhance trust and confidence in information security12. References = CISM Review Manual (Digital Version), Chapter 1: Information Security Governance CISM Review Manual (Print Version), Chapter 1: Information Security Governance

NEW QUESTION: 311
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: A (LEAVE A REPLY)
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: 312
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: A (LEAVE A REPLY)
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: 313
Which of the following is MOST effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application?
A. A patch management process
B. Version control
C. Change management controls
D. Logical access controls
Answer: A (LEAVE A REPLY)
= Change management controls are the most effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application. Change management controls are the policies, procedures, and practices that govern the initiation, approval, implementation, testing, and documentation of changes to the information systems and infrastructure. Change management controls help to ensure that changes are authorized, planned, controlled, and monitored, and that they do not introduce any unintended or adverse effects on the security, functionality, performance, or reliability of the system or application. Change management controls also help to identify and mitigate any potential risks or issues that may arise from the changes, and to ensure that the changes are aligned with the business objectives and requirements. By implementing change management controls, the organization can prevent the introduction of vulnerabilities that may disrupt the availability of a critical business application, as well as enhance the quality and efficiency of the change process. References = CISM Review Manual 15th Edition, page 105, page 106.

NEW QUESTION: 314
A balanced scorecard MOST effectively enables information security:
A. risk management
B. project management
C. governance

D. performance

Answer: C (LEAVE A REPLY)

A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it. A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2. It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

NEW QUESTION: 315

During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption, unauthorized alterations, and errors?

A. Configuration management

B. Password management

C. Change management

D. Version management

Answer: C (LEAVE A REPLY)

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

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

NEW QUESTION: 316

An organization has been penalized by regulatory authorities for failing to notify them of a major security breach that may have compromised customer data. Which of the following is MOST likely in need of review and updating to prevent similar penalties in the future?

A. Incident communication plan

B. Information security policies and procedures

C. Business continuity plan (BCP)

D. Incident response training program

Answer: (SHOW ANSWER)

NEW QUESTION: 317
An information security manager has learned of an increasing trend in attacks that use phishing emails impersonating an organization's CEO in an attempt to commit wire transfer fraud. Which of the following is the BEST way to reduce the risk associated with this type of attack?
A. Temporarily suspend wire transfers for the organization.
B. Provide awareness training to staff responsible for wire transfers.
C. Provide awareness training to the CEO for this type of phishing attack.
D. Disable emails for staff responsible for wire transfers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 318
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: D (LEAVE A REPLY)
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.

NEW QUESTION: 319
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: B (LEAVE A REPLY)
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: 320
Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?
A. To identify the organization's risk tolerance
B. To improve security processes
C. To align security roles and responsibilities
D. To optimize security risk management
Answer: D (LEAVE A REPLY)
= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By aligning information security with the organization's

strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner1. Alignment also enables the information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives2. Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability3. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information assets with the business objectives and risk appetite of the organization4. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

NEW QUESTION: 321
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: 322
Business objectives and organizational risk appetite are MOST useful inputs to the development of information security:
A. key performance indicators (KPIs).
B. risk assessments.
C. standards.
D. strategy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 323
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: B (LEAVE A REPLY)
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: 324
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: 325
Which is following should be an information security manager's PRIMARY focus during the development of a critical system storing highly confidential data?
A. Reducing the number of vulnerabilities detected
B. Ensuring the amount of residual risk is acceptable
C. Avoiding identified system threats
D. Complying with regulatory requirements

Answer: B (LEAVE A REPLY)
The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable. Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

NEW QUESTION: 326
Which of the following provides the MOST effective response against ransomware attacks?
A. Automatic quarantine of systems
B. Thorough communication plans
C. Effective backup plans and processes
D. Strong password requirements
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Recovering from ransomware attacks often depends on having a robust data recovery strategy:
A). Automatic quarantine of systems: This can limit the spread of ransomware but does not address recovery.
B). Thorough communication plans: Communication is important during incidents but does not directly mitigate ransomware.
C). Effective backup plans and processes: This is the BEST option because having backups ensures that encrypted data can be restored, minimizing downtime and data loss.
D). Strong password requirements: This helps prevent unauthorized access but is not sufficient to combat ransomware once it has entered the system.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) stresses the importance of backup and recovery strategies to mitigate ransomware risks.

NEW QUESTION: 327
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: 328
Which of the following should be done FIRST to prioritize response to incidents?
A. Escalation
B. Containment
C. Analysis
D. Triage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 329
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: C (LEAVE A REPLY)

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: 330
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: A (LEAVE A REPLY)
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: 331
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: D (LEAVE A REPLY)
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: 332
What should be an information security manager's FIRST course of action upon learning a business unit is bypassing an existing control in order to increase operational efficiency?
A. Report the noncompliance to senior management.
B. Assess the risk of noncompliance.
C. Activate the incident response plan.
D. Evaluate possible compensating controls.
Answer: B (LEAVE A REPLY)
Assessing the risk of noncompliance ensures that decisions are based on an understanding of the business impact and security implications.
"Before reporting or remediating, it is critical to assess the risk associated with the control bypass to make informed decisions."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment*

NEW QUESTION: 333
An information security manager has confirmed the organization's cloud provider has unintentionally published some of the organization's business data. Which of the following should be done NEXT?
A. Invoke the incident response plan.
B. Identify users associated with the exposed data.
C. Review the cloud provider's service level agreement (SLA).
D. Initiate the organization's data loss prevention (DLP) processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 334

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: 335

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: C (LEAVE A REPLY)

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: 336
Which of the following should be the PRIMARY focus of a lessons learned exercise following a successful response to a cybersecurity incident?
A. Establishing the root cause of the incident
B. Identifying attack vectors utilized in the incident
C. When business operations were restored after the incident
D. How incident management processes were executed
Answer: D (LEAVE A REPLY)
The primary focus of a lessons learned exercise following a successful response to a cybersecurity incident is to evaluate how the incident management processes were executed, and to identify the strengths, weaknesses, best practices, and improvement opportunities for future incidents. A lessons learned exercise is not meant to determine the root cause, the attack vectors, or the recovery time of the incident, but rather to assess the performance and effectiveness of the incident response team and the incident response plan.
References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "How incident management processes were executed is the correct answer because it is the primary focus of a lessons learned exercise, which aims to evaluate the incident response capability and to implement corrective actions and improvement plans" (p. 97). Additionally, the Cybersecurity Incident Response Exercise Guidance article from the ISACA Journal 2022 states that "The AAR [after-action review] should include the date and time of the exercise, a list of participants, scenario descriptions, findings (generic and specific), observations with recommendations, lessons learned and an evaluation of the exercise (strengths, weaknesses, lessons learned)" (p. 3)1

NEW QUESTION: 337
When remote access is granted to a company's internal network, the MOST important consideration should be that access is provided:
A. by the use of a remote access server.
B. if a robust IT infrastructure exists.
C. on a need-to-know basis subject to controls.
D. subject to legal and regulatory requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 338

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: 339
Which of the following is the PRIMARY objective of testing security controls within a critical infrastructure?
A. Ensuring the continued resilience and security of IT services
B. Decreasing the percentage of security deployments that cause failures in production
C. Identifying and addressing security team performance issues
D. Reducing the number of control assessments to optimize resources
Answer: (SHOW ANSWER)

NEW QUESTION: 340
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: 341
What should be an information security manager's MOST important consideration when developing a multi- year plan?
A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year
Answer: (SHOW ANSWER)
= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its various units. Alignment also means that the information security plan is consistent and compatible with the plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .
By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :
Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization's performance, growth, and competitiveness. The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization's assets, processes, and activities.
Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also

foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.
Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.
The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive and enabling aspects. Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization's needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization's financial situation or expectations1 . References = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk Management (IRM) [2022 update], Aligning Information Security with Business Strategy - ISACA, [Aligning Information Security with Business Objectives - ISACA]

NEW QUESTION: 342
Which of the following is the MOST important reason for an information security manager to archive and retain the organization's electronic communication and email data?
A. To track personal use of electronic communication by users
B. To provide as evidence in legal proceedings when required
C. To meet the requirements of global security standards
D. To identify and scan attachments for malware
Answer: B (LEAVE A REPLY)
Retaining communications ensures the organization can produce evidence for litigation or regulatory investigations, which is often a legal obligation.

"Organizations must retain electronic communications to support legal discovery, compliance audits, and investigative needs."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Requirements*

NEW QUESTION: 343
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?
A. Employee training on ransomware
B. A properly tested offline backup system
C. A continual server replication process
D. A properly configured firewall
Answer: B (LEAVE A REPLY)
The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures.
Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware.
However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable.
A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 344
The PRIMARY goal to a post-incident review should be to:
A. identify policy changes to prevent a recurrence.
B. determine how to improve the incident handling process.
C. establish the cost of the incident to the business.

D. determine why the incident occurred.

Answer: B (LEAVE A REPLY)

The primary goal of a post-incident review is to identify areas for improvement in the incident handling process. The focus is on evaluating the effectiveness of incident response procedures, technical controls, communication channels, coordination among teams, documentation, and any other relevant aspects. The post- incident review should also provide recommendations for corrective actions, preventive measures, and lessons learned that can help reduce the likelihood and impact of future incidents12. References = CISM Review Manual 15th Edition, page 1251; CISM Item Development Guide, page 72

NEW QUESTION: 345

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: C (LEAVE A REPLY)

Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks.

Therefore, conducting awareness training across the organization is the correct answer.

References:

https://almanac.upenn.edu/articles/one-step-ahead-dont-get-caught-by-targeted-email-attacks

https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html

NEW QUESTION: 346

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

A. Nonrepudiation

B. Authenticity

C. Availability

D. Recovery time objective (RTO)

Answer: C (LEAVE A REPLY)

= 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: 347

Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Require remote wipe capabilities for devices.

B. Conduct security awareness training.

C. Review and update existing security policies.

D. Enforce passwords and data encryption on the devices.

Answer: C (LEAVE A REPLY)

The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation's security program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be reviewed and updated regularly to reflect changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities,

as well as new opportunities and benefits, for the organiza-tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:
*The scope, purpose, and ownership of company-owned mobile devices
*The acceptable and unacceptable use of company-owned mobile devices
*The security standards and best practices for company-owned mobile devices
*The roles and responsibilities of users, managers, IT staff, and vendors regarding compa-ny-owned mobile devices
*The procedures for provisioning, managing, monitoring, and decommissioning company-owned mobile devices
*The incident response and reporting process for company-owned mobile devices By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com-promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices.
References:
1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is
& How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

NEW QUESTION: 348
Which of the following is the MOST effective way to demonstrate alignment of information security strategy with business objectives?
A. Balanced scorecard
B. Risk matrix
C. Benchmarking
D. Heat map
Answer: (SHOW ANSWER)
The most effective way to demonstrate alignment of information security strategy with business objectives is to use a balanced scorecard. A balanced scorecard is a strategic management tool that translates the vision and mission of an organization into a set of performance indicators that measure its progress towards its goals. A balanced scorecard

typically includes four perspectives: financial, customer, internal process, and learning and growth. Each perspective has a set of objectives, measures, targets, and initiatives that are aligned with the organization's strategy. A balanced scorecard helps to communicate, monitor, and evaluate the performance of the organization and its information security program in relation to its business objectives. A balanced scorecard also helps to identify and prioritize improvement opportunities, as well as to align the activities and resources of the organization with its strategy12.

The other options are not the most effective ways to demonstrate alignment of information security strategy with business objectives. A risk matrix is a tool that displays the likelihood and impact of various risks on a two-dimensional grid. A risk matrix helps to assess and prioritize risks, as well as to determine the appropriate risk response strategies. However, a risk matrix does not show how the information security strategy supports the business objectives, nor does it measure the performance or the value of the information security program3. Benchmarking is a process of comparing the performance, practices, or processes of an organization with those of other organizations or industry standards. Benchmarking helps to identify best practices, gaps, and areas for improvement, as well as to set realistic and achievable goals. However, benchmarking does not show how the information security strategy aligns with the business objectives, nor does it reflect the unique characteristics and needs of the organization4. A heat map is a graphical representation of data using colors to indicate the intensity or frequency of a variable. A heat map can be used to visualize the distribution, concentration, or variation of risks, controls, or incidents across different dimensions, such as business units, processes, or assets. A heat map helps to highlight the areas of high risk or low control effectiveness, as well as to facilitate decision making and resource allocation. However, a heat map does not show how the information security strategy contributes to the business objectives, nor does it measure the outcomes or the benefits of the information security program5.

References = CISM Review Manual, 16th Edition | Print | English 2, Chapter 1: Information Security Governance, pages 28-
29, 31-32, 34-35.
Balanced Scorecard - Wikipedia 1
Risk Matrix - Wikipedia 3
Benchmarking - Wikipedia 4
Heat map - Wikipedia 5

NEW QUESTION: 349

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. Revise the policy to accommodate the business unit.

B. Report the business unit for policy noncompliance.

C. Review the business unit's function against the policy.

D. Enforce sanctions on the business unit.

Answer: C (LEAVE A REPLY)

The best first step is to review the business unit's function against the policy to determine why violations are occurring-e.g., misalignment with business processes, unclear requirements, infeasible controls, poor communication, or lack of enabling procedures/standards. In CISM governance, policies must be business- aligned, implementable, and supported by standards and processes. Jumping directly to sanctions (D) or reporting noncompliance (B) may be necessary later, but those are enforcement actions that should follow root-cause identification and confirmation that expectations were properly communicated, understood, and achievable. Revising the policy to "accommodate" violations (A) is generally weak governance unless analysis shows the policy truly conflicts with legitimate business needs and risk appetite. By comparing the unit's operational reality to the policy intent, the security manager can identify control gaps, training needs, process exceptions, or required compensating controls-then escalate appropriately if willful noncompliance persists.

References: ISACA CISM Review Manual (Information Security Governance-policy framework, alignment with business objectives, enforcement approach); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 350

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: 351

Which of the following documents should contain the INITIAL prioritization of recovery of services?

A. IT risk analysis
B. Threat assessment
C. Business impact analysis (BIA)
D. Business process map
Answer: C (LEAVE A REPLY)
A business impact analysis (BIA) is the document that should contain the initial prioritization of recovery of services. A BIA is a process of identifying and analyzing the potential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:
*Identifying the critical business functions and processes that support the organization's mission and objectives.
*Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.
*Assessing the potential impacts of disruptions to each function or process, such as financial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatisfaction, etc.
*Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.
*Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.
A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or recovery of critical business functions and processes in the event of a disruption2. The other options are not documents that should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3.
A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes.
References: 1:
Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process mapping - Wikipedia

NEW QUESTION: 352
Which of the following presents the GREATEST challenge to a security operations center's wna GY of potential security breaches?
A. IT system clocks are not synchronized with the centralized logging server.
B. Operating systems are no longer supported by the vendor.
C. The patch management system does not deploy patches in a timely manner.
D. An organization has a decentralized data center that uses cloud services.
Answer: (SHOW ANSWER)
A security operations center (SOC) relies on the centralized logging server to collect, store, analyze and correlate security events from various sources such as firewalls, intrusion detection systems, antivirus software, etc. The centralized logging server uses the timestamps of the events to perform the analysis and correlation. If the IT system clocks are not synchronized with the centralized logging server, the SOC will face difficulties in identifying the sequence and causality of the events, which will affect its ability to detect and respond to potential security breaches. Therefore, this presents the greatest challenge to the SOC's awareness of potential security breaches.
Operating systems that are no longer supported by the vendor may pose a security risk, but they can be mitigated by applying compensating controls such as isolation, segmentation, monitoring, etc. The patch management system that does not deploy patches in a timely manner may also increase the vulnerability exposure, but it can be remediated by prioritizing and applying the critical patches as soon as possible. An organization that has a decentralized data center that uses cloud services may face some challenges in ensuring the security and compliance of the cloud environment, but it can leverage the cloud service provider' s security capabilities and tools to enhance the SOC's visibility and control. Therefore, these options are not the greatest challenges to the SOC's awareness of potential security breaches. References = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page
2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; RSI Security, Common Challenges of SOC Teams3; Infosec Matter, Security Operations Center: Challenges of SOC Teams4

NEW QUESTION: 353
Which of the following would BEST address the risk of a system failing to detect a breach?
A. User access reviews
B. Log monitoring
C. Vulnerability scanning
D. Security control testing
Answer: B (LEAVE A REPLY)

Log monitoring (B) directly addresses the risk of a system failing to detect a breach by enabling continuous visibility into system activity, anomalies, and indicators of compromise. CISM emphasizes detection as a critical component of incident management, with log review and monitoring serving as primary detective controls. User access reviews (A) are preventive and periodic, not real-time. Vulnerability scanning (C) identifies weaknesses but does not detect active breaches. Security control testing (D) validates control design and effectiveness but does not provide ongoing breach detection. Effective log monitoring reduces mean time to detect incidents and limits business impact. References: ISACA CISM Review Manual (Incident management-detection and monitoring); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 354
To help ensure that an information security training program is MOST effective its contents should be
A. focused on information security policy.
B. aligned to business processes
C. based on employees' roles
D. based on recent incidents
Answer: C (LEAVE A REPLY)
"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

NEW QUESTION: 355
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: B (LEAVE A REPLY)
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: 356
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: D (LEAVE A REPLY)
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: 357
Which of the following is the MOST effective way to increase security awareness in an organization?
A. Implement regularly scheduled information security audits.
B. Conduct periodic simulated phishing exercises.
C. Require signed acknowledgment of information security policies.
D. Include information security requirements in job descriptions.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 358
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: A (LEAVE A REPLY)
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.

NEW QUESTION: 359
Which of the following should be the PRIMARY basis for an information security strategy?
A. The organization's vision and mission
B. Results of a comprehensive gap analysis
C. Information security policies
D. Audit and regulatory requirements
Answer: A (LEAVE A REPLY)
The organization's vision and mission should be the PRIMARY basis for an information security strategy, as they define the purpose and direction of the organization and its information security needs. A comprehensive gap analysis is a tool to identify the current state and desired state of information security, and the actions needed to close the gap. Information security policies are the high-level statements of management's intent and expectations for information security, and are derived from the information security strategy. Audit and regulatory requirements are external factors that influence the information security strategy, but are not the primary basis for it. References = CISM Review Manual, 16th Edition, pages 17-181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 782 The primary basis for an information security strategy should be the organization's vision and mission. The organization's vision and mission should be the foundation for the security strategy, and should inform and guide the security policies, procedures, and practices that are implemented. The results of a comprehensive gap analysis, information security policies, and audit and regulatory requirements should all be taken into consideration when developing the security strategy, but should not be the primary basis.

NEW QUESTION: 360
When deciding to move to a cloud-based model, the FIRST consideration should be:
A. storage in a shared environment.
B. availability of the data.
C. data classification.
D. physical location of the data.
Answer: C (LEAVE A REPLY)
The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.
Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co- located with other customers' data, and may be subject to unauthorized access, modification, or deletion.
Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies.
However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment.
References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

NEW QUESTION: 361
Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?
A. Impact on information security program
B. Cost of controls
C. Impact to business function
D. Cost to replace
Answer: C (LEAVE A REPLY)

The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.
Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset. Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization.
References = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693 When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture. Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

NEW QUESTION: 362
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: 363
Which of the following BEST indicates that an information security governance framework has been successfully implemented?
A. The framework aligns internal and external resources.
B. The framework aligns security processes with industry best practices.
C. The framework aligns management and other functions within the security organization.
D. The framework includes commercial off-the-shelf security solutions.
Answer: A (LEAVE A REPLY)
The best indicator that an information security governance framework has been successfully implemented is A: The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.
The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

NEW QUESTION: 364
Which or the following is MOST important to consider when determining backup frequency?
A. Recovery point objective (RPO)
B. Allowable interruption window
C. Recovery time objective (RTO)
D. Maximum tolerable outage (MTO)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 365
What is the PRIMARY objective of implementing standard security configurations?
A. Maintain a flexible approach to mitigate potential risk to unsupported systems.
B. Minimize the operational burden of managing and monitoring unsupported systems.
C. Control vulnerabilities and reduce threats from changed configurations.
D. Compare configurations between supported and unsupported systems.
Answer: C (LEAVE A REPLY)
The primary objective of implementing standard security configurations is to control vulnerabilities and reduce threats from changed configurations. Standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices. By implementing standard security configurations, the organization can ensure that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected. This can help to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should establish and implement standard security configurations for information systems and devices, and monitor and review the security configuration on a regular basis and take corrective actions when deviations or violations are detected" (p.
138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Control vulnerabilities and reduce threats from changed configurations is the correct answer because it is the primary objective of implementing standard security configurations, as it helps to maintain the security posture and functionality of information systems and devices, and to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks" (p. 63). Additionally, the article Standard Security Configurations from the ISACA Journal 2017 states that "standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices" and that "standard security configurations can help to control vulnerabilities and reduce threats from changed configurations by ensuring that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected" (p. 1)

NEW QUESTION: 366
Which of the following is MOST important for building 4 robust information security culture within an organization?
A. Mature information security awareness training across the organization

B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies
Answer: (SHOW ANSWER)
= Mature information security awareness training across the organization is the most important factor for building a robust information security culture, because it helps to educate and motivate the employees to understand and adopt the security policies, procedures, and best practices that are aligned with the organizational goals and values. Information security awareness training should be tailored to the specific roles, responsibilities, and needs of the employees, and should cover the relevant topics, such as:
The importance and value of information assets and the potential risks and threats to them The legal, regulatory, and contractual obligations and compliance requirements related to information security The organizational security policies, standards, and guidelines that define the expected and acceptable behaviors and actions regarding information security The security controls and tools that are implemented to protect the information assets and how to use them effectively and efficiently The security incidents and breaches that may occur and how to prevent, detect, report, and respond to them The security best practices and tips that can help to enhance the security posture and culture of the organization Information security awareness training should be delivered through various methods and channels, such as:
Online courses, webinars, videos, podcasts, and quizzes that are accessible and interactive Classroom sessions, workshops, seminars, and simulations that are engaging and practical Posters, flyers, newsletters, emails, and social media that are informative and catchy Games, competitions, rewards, and recognition that are fun and incentivizing Information security awareness training should be conducted regularly and updated frequently, to ensure that the employees are aware of the latest security trends, challenges, and solutions, and that they can demonstrate their knowledge and skills in a consistent and effective manner.
Mature information security awareness training can help to create a positive and proactive security culture that fosters trust, collaboration, and innovation among the employees and the organization, and that supports the achievement of the strategic objectives and the mission and vision of the organization.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 144-146, 149-150.

NEW QUESTION: 367
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: A (LEAVE A REPLY)
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: 368
Which of the following is MOST important to convey to employees in building a security risk-aware culture?
A. Personal information requires different security controls than sensitive information.
B. Employee access should be based on the principle of least privilege.
C. Understanding an information asset's value is critical to risk management.
D. The responsibility for security rests with all employees.
Answer: (SHOW ANSWER)
= The most important message to convey to employees in building a security risk-aware culture is that the responsibility for security rests with all employees, not just the information security function or the management. A security risk-aware culture is a collective mindset of the people in the organization working every day to protect the enterprise and its information assets from internal and external threats. A security risk-aware culture requires the workforce to know the security risks and the processes for avoiding or mitigating them, and to make thoughtful decisions that align with security policies and standards. A security risk-aware culture also incorporates a broader corporate

culture of day-to-day actions that encourage employees to report security incidents, share security best practices, and participate in security awareness and training programs.
A security risk-aware culture helps to reduce the human factor that causes 90 percent of all cyberattacks, and to offset the impact of corrupted or lost data, decreased revenue, regulatory fines, and reputational damage. A security risk-aware culture turns people from assets that must be protected into assets that actively contribute to the cybersecurity and risk management posture and elevate security to being a business enabler rather than a business impediment123.
Personal information requires different security controls than sensitive information is a true statement, but it is not the most important message to convey to employees in building a security risk-aware culture. Personal information is any information that can identify or relate to a natural person, such as name, address, email, phone number, social security number, etc. Sensitive information is any information that is confidential, proprietary, or has a high value or impact to the organization, such as trade secrets, financial data, customer data, intellectual property, etc. Different types of information may have different legal, regulatory, contractual, or ethical obligations to protect them from unauthorized access, use, disclosure, modification, or destruction. Therefore, different security controls may be applied to personal and sensitive information based on their classification, such as encryption, access control, retention, disposal, etc. However, this message does not address the broader concept of security risk-aware culture, which is not limited to information classification and protection, but also encompasses the behaviors, attitudes, and values of the employees towards security.
Employee access should be based on the principle of least privilege is a good practice, but it is not the most important message to convey to employees in building a security risk-aware culture. The principle of least privilege states that users should only have the minimum level of access and permissions that are necessary to perform their job functions, and no more. This principle helps to reduce the risk of unauthorized or inappropriate actions, such as data leakage, fraud, sabotage, etc., by limiting the exposure and impact of user activities. However, this message does not capture the essence of security risk-aware culture, which is not only about access control, but also about the awareness, understanding, and commitment of the employees to security.
Understanding an information asset's value is critical to risk management is a valid point, but it is not the most important message to convey to employees in building a security risk-aware culture. Understanding an information asset's value is essential to determine the potential impact and likelihood of a security risk, and to prioritize the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
However, this message does not reflect the holistic nature of security risk-aware culture, which is not only about risk assessment, but also about risk communication, risk treatment, and risk monitoring. References = Building a Culture of Security - ISACA2 The Risk-Conscious, Security-Aware Culture: The Forgotten Critical Security Control - Cisco3 CISM ITEM DEVELOPMENT GUIDE - ISACA4

NEW QUESTION: 369
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: 370
From an information security perspective, legal issues associated with a transborder flow of technology- related items are MOST often
A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.

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

NEW QUESTION: 371
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: C (LEAVE A REPLY)
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.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

NEW QUESTION: 372
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: D (LEAVE A REPLY)
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: 373
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: D (LEAVE A REPLY)
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.

NEW QUESTION: 374
Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?
A. Tabletop exercises
B. Forensics certification
C. Penetration tests
D. Disaster recovery drills
Answer: (SHOW ANSWER)

NEW QUESTION: 375
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: B (LEAVE A REPLY)
= 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: 376
Which of the following is the BEST way lo monitor for advanced persistent threats (APT) in an organization?
A. Network with peers in the industry to share information.
B. Browse the Internet to team of potential events
C. Search for anomalies in the environment
D. Search for threat signatures in the environment.
Answer: (SHOW ANSWER)
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: 377
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: 378
The resilience requirements of an application are BEST determined by:
A. A risk assessment
B. A business impact analysis (BIA)
C. A cost-benefit analysis
D. A threat assessment
Answer: B (LEAVE A REPLY)
A business impact analysis (BIA) (B) best determines application resilience requirements because it identifies criticality, maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs) based on business impact. Resilience is fundamentally about the organization's ability to continue or rapidly restore critical business functions. Risk assessments (A) and threat assessments (D) identify risks and threat sources but do not define acceptable downtime or recovery priorities. Cost- benefit analysis (C) helps evaluate investment decisions but is secondary to understanding business impact.

CISM clearly positions the BIA as the foundation for continuity, resilience, and recovery planning decisions, ensuring security and availability controls align with business priorities. References: ISACA CISM Review Manual (Risk management-BIA, resilience, continuity planning); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 379
Which of the following will result in the MOST accurate controls assessment?
A. Mature change management processes
B. Senior management support
C. Well-defined security policies
D. Unannounced testing
Answer: D (LEAVE A REPLY)
Unannounced testing is the most accurate way to assess the effectiveness of controls, as it simulates a real- world scenario and does not allow the staff to prepare or modify their behavior in advance. Mature change management processes, senior management support, and well-defined security policies are all important factors for establishing and maintaining a strong security posture, but they do not directly measure the performance of controls. References = CISM Review Manual, 16th Edition, page 149. CISM Questions, Answers & Explanations Database, question ID 1003.

NEW QUESTION: 380
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: A (LEAVE A REPLY)
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: 381
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: B (LEAVE A REPLY)
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus primarily on defining security requirements for the process being outsourced.
Security requirements are the specifications of what needs to be done to protect the information assets from unauthorized access, use, disclosure, modification, or destruction. Security requirements should be aligned with the organization's risk appetite and business objectives, and should cover both technical and organizational aspects of the service delivery. Security requirements should also be clear, concise, measurable, achievable, realistic, and testable. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information.
They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are essential to protect the information assets of the organization and to establish a clear and en-forceable contractual relationship with the third party.
References:
*1 Outsourcing Strategies for Information Security: Correlated Losses and Security Exter-nalities - SpringerLink
*2 What requirements must outsourcing services comply with for the European market? - CBI
*3 Outsourcing cybersecurity: What services to outsource, what to keep in house - Infosec Institute
*4 BCFSA outsourcing and information security guidelines - BLG

NEW QUESTION: 382
An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?
A. Implementing automated vulnerability scanning in the help desk workflow

B. Changing the default setting for all security incidents to the highest priority
C. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system
D. Integrating incident response workflow into the help desk ticketing system
Answer: D (LEAVE A REPLY)
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: 383
Which of the following should be updated FIRST when aligning the incident response plan with the corporate strategy?
A. Disaster recovery plan (DRP)
B. Incident notification plan
C. Risk response scenarios
D. Security procedures
Answer: (SHOW ANSWER)
The answer to the question is C. Risk response scenarios. This is because risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents, such as cyberattacks, natural disasters, or data breaches. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization, and guides the decision- making and resource allocation processes. By aligning the risk response scenarios with the corporate strategy, the organization can ensure that the incident response plan supports the achievement of the desired outcomes and benefits, and minimizes the impact and disruption to the business operations and performance.
Risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2111; CISM domain 4: Information security incident management [2022 update] | Infosec2; A Guide to Effective Incident Management Communications3

NEW QUESTION: 384
Information security controls should be designed PRIMARILY based on:
A. a business impact analysis (BIA).
B. regulatory requirements.
C. business risk scenarios,
D. a vulnerability assessment.
Answer: C (LEAVE A REPLY)
Information security controls should be designed primarily based on business risk scenarios, because they help to identify and prioritize the most relevant and significant threats and vulnerabilities that may affect the organization's information assets and business objectives. Business risk scenarios are hypothetical situations that describe the possible sources, events, and consequences of a security breach, as well as the likelihood and impact of the occurrence. Business risk scenarios can help to:
Align the information security controls with the business needs and requirements, and ensure that they support the achievement of the strategic goals and the mission and vision of the organization Assess the effectiveness and efficiency of the existing information security controls, and identify the gaps and weaknesses that need to be addressed or improved Select and implement the appropriate information security controls that can prevent, detect, or mitigate the risks, and that can provide the optimal level of protection and performance for the information assets Evaluate and measure the return on investment and the value proposition of the information security controls, and communicate and justify the rationale and benefits of the controls to the stakeholders and management
Information security controls should not be designed primarily based on a business impact analysis (BIA), regulatory requirements, or a vulnerability assessment, because these are secondary or complementary factors that influence the design of the controls, but they do not provide the main basis or criteria for the design. A BIA is a method of estimating and comparing the potential effects of a disruption or a disaster on the critical business functions and processes, in terms of financial, operational, and reputational aspects. A BIA can help to determine the recovery objectives and priorities for the information assets, but it does not identify or address the specific risks and threats that may cause the disruption or the disaster. Regulatory requirements are the legal, contractual, or industry standards and obligations that the organization must comply with regarding information security. Regulatory requirements can help to establish the minimum or baseline level of information security controls that the organization must implement, but they do not reflect the specific or unique needs and challenges of the organization. A vulnerability assessment is a method of identifying and analyzing the weaknesses and flaws in the information systems and assets that may expose them to exploitation or compromise. A vulnerability assessment can help to discover and remediate the existing or potential security issues, but it does not consider the business context or impact of the issues.

References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 119-120, 122-123, 125-126, 129-130.

NEW QUESTION: 385
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: 386
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: D (LEAVE A REPLY)
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: 387
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: B (LEAVE A REPLY)
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: 388
An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:
A. a control self-assessment (CSA) process.
B. automated reporting to stakeholders.
C. a monitoring process for the security policy.
D. metrics for each milestone.
Answer: D (LEAVE A REPLY)
= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress, performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.
The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self- assessment (CSA) process is a technique to involve the staff in assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and

decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.
CISM domain 1: Information security governance [Updated 2022], Infosec, 1.
Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

NEW QUESTION: 389
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 separation of duties is maintained
C. To ensure system audit trails are not bypassed
D. To prevent unauthorized user access
Answer: (SHOW ANSWER)

NEW QUESTION: 390
Which of the following BEST enables an organization to maintain legally admissible evidence7
A. Documented processes around forensic records retention
B. Robust legal framework with notes of legal actions
C. Chain of custody forms with points of contact
D. Forensic personnel training that includes technical actions
Answer: (SHOW ANSWER)
Chain of custody forms with points of contact are the best way to enable an organization to maintain legally admissible evidence because they document the sequence of control, transfer, and analysis of the evidence, and every person who handled it, the dates and times, and the purpose for each action1. They also ensure the authenticity and integrity of the evidence, and prevent tampering or loss1. Documented processes around forensic records retention are not sufficient to maintain legally admissible evidence because they

do not track or verify the handling of the evidence. Robust legal framework with notes of legal actions are not sufficient to maintain legally admissible evidence because they do not record or validate the preservation of the evidence. Forensic personnel training that includes technical actions are not sufficient to maintain legally admissible evidence because they do not account or certify the custody of the evidence.
References: 1
https://www.researchgate.net/publication/326079761_Digital_Chain_of_Custody

NEW QUESTION: 391
Which of the following BEST minimizes information security risk in deploying applications to the production environment?
A. Integrating security controls in each phase of the life cycle
B. Conducting penetration testing post implementation
C. Having a well-defined change process
D. Verifying security during the testing process
Answer: A (LEAVE A REPLY)
= Integrating security controls in each phase of the life cycle is the best way to minimize information security risk in deploying applications to the production environment. This ensures that security requirements are defined, designed, implemented, tested, and maintained throughout the development process. Conducting penetration testing post implementation, having a well-defined change process, and verifying security during the testing process are all important activities, but they are not sufficient to address all the potential risks that may arise during the application life cycle. Penetration testing may reveal some vulnerabilities, but it cannot guarantee that all of them are identified and fixed. A change process may help to control and document the modifications made to the application, but it does not ensure that the changes are secure and do not introduce new risks. Verifying security during the testing process may help to validate the functionality and performance of the security controls, but it does not ensure that the security requirements are complete and consistent with the business objectives and the risk appetite of the organization. References = CISM Review Manual, 16th Edition, page 1121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462

NEW QUESTION: 392
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: C (LEAVE A REPLY)
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: 393
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/

NEW QUESTION: 394
Which of the following is an information security manager's BEST course of action when a penetration test reveals a security exposure due to a firewall that is not configured correctly?
A. Ensure a plan with milestones is developed.
B. Implement a distributed denial of service (DDoS) control.
C. Engage the incident response team.
D. Define new key performance indicators (KPIs).
Answer: A (LEAVE A REPLY)
A penetration test is a proactive way to identify and remediate security vulnerabilities in a network. When a penetration test reveals a security exposure due to a firewall that is not configured correctly, the information security manager's best course of action is to ensure a plan with milestones is developed to address the issue.
This plan should include the root cause analysis, the corrective actions, the responsible parties, the deadlines, and the verification methods. This way, the information security manager can ensure that the security exposure is resolved in a timely and effective manner, and that the firewall configuration is aligned with the security policy and the business objectives.
References =
CISM Review Manual (Digital Version), page 193: "The information security manager should ensure that a plan with milestones is developed to address the issues identified during the penetration test." How to configure a network firewall: Walkthrough: "A good network firewall is essential. Learn the basics of configuring a network firewall, including stateful vs. stateless firewalls and access control lists in this episode of Cyber Work Applied." Which of the following is the BEST way to evaluate whether the information security program aligns with corporate governance?
A). Survey mid-level management.
B). Analyze industry benchmarks.
C). Conduct a gap analysis.
D). Review internal audit reports.

NEW QUESTION: 395
Which of the following would BEST justify continued investment in an information security program?
A. Reduction in residual risk
B. Security framework alignment
C. Speed of implementation
D. Industry peer benchmarking
Answer: A (LEAVE A REPLY)

Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. References = CISM Review Manual, 16th Edition, page 431; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 622 Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

NEW QUESTION: 396
Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?
A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats
Answer: B (LEAVE A REPLY)
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

NEW QUESTION: 397
A user reports a stolen personal mobile device that stores sensitive corporate data. Which of the following will BEST minimize the risk of data exposure?
A. Prevent the user from using personal mobile devices.
B. Report the incident to the police.
C. Wipe the device remotely.
D. Remove user's access to corporate data.
Answer: C (LEAVE A REPLY)
Wiping the device remotely is the best option to minimize the risk of data exposure from a stolen personal mobile device. This action will erase all the data stored on the device, including the sensitive corporate data, and prevent unauthorized access or misuse. Wiping

the device remotely can be done using enterprise mobility management (EMM) or mobile device management (MDM) tools that allow administrators to remotely manage and secure mobile devices. Alternatively, some mobile devices have built-in features that allow users to wipe their own devices remotely using another device or a web portal.
Preventing the user from using personal mobile devices is not a feasible option, as it may affect the user's productivity and convenience. Moreover, this option does not address the immediate risk of data exposure from the stolen device.
Reporting the incident to the police is a good practice, but it does not guarantee that the device will be recovered or that the data will be protected. The police may not have the resources or the authority to track down the device or access it.
Removing the user's access to corporate data is a preventive measure that can limit the damage caused by a stolen device, but it does not eliminate the risk of data exposure from the data already stored on the device.
The user may have cached or downloaded data that can still be accessed by an attacker even if the user's access is revoked. References = Guidelines for Managing the Security of Mobile Devices in the Enterprise NIST Special Publication, Section
3.1.11, page 3-8
CISM Review Manual, Chapter 3, page 121
Mobile device security - CISM Certification Domain 2: Information Risk Management Video Boot Camp
2019, Section 3.3, 00:03:10

NEW QUESTION: 398
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. Periodically change risk awareness messages.
D. Ensure that threats are documented and communicated in a timely manner.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 399
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: C (LEAVE A REPLY)
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: 400
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: C (LEAVE A REPLY)
= 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: 401
Which of the following is the GREATEST benefit of using AI tools in security operations?
A. Rapid detection and response to threats
B. Prioritized vulnerabilities
C. Reduced time and effort required to patch systems
D. Defined risk tolerance
Answer: (SHOW ANSWER)
AI-driven tools enable real-time analysis, anomaly detection, and automated response, drastically reducing the time to identify and respond to threats. This capability is particularly effective against advanced persistent threats (APTs) and zero-day exploits.
"AI tools enhance security operations by enabling rapid threat detection and incident response, often before traditional tools can react."
- CISM Review Manual 15th Edition, Chapter 4: Security Operations and Threat Intelligence* Other benefits (e.g., prioritization or patching) are secondary compared to the speed and precision of AI-based threat response.

NEW QUESTION: 402
Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?
A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider
Answer: D (LEAVE A REPLY)
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider.
References:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a- long-outage/

https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117- p599mr

NEW QUESTION: 403
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: 404
Which of the following is PRIMARILY determined by asset classification?
A. Insurance coverage required for assets
B. Level of protection required for assets
C. Priority for asset replacement
D. Replacement cost of assets
Answer: B (LEAVE A REPLY)
Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. References = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

NEW QUESTION: 405
Which of the following should be updated FIRST to account for new regulatory requirements that impact current information security controls?
A. Control matrix
B. Business impact analysis (BIA)
C. Risk register
D. Information security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 406
What should an information security manager do FIRST when an organization is planning to use a third-party cloud computing service for a critical business process?
A. Perform a gap analysis.
B. Perform a risk assessment.
C. Identify the data to be hosted.
D. Analyze the business requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 407
Which of the following BEST enables an organization to transform its culture to support information security?
A. Periodic compliance audits
B. Strong management support
C. Robust technical security controls
D. Incentives for security incident reporting
Answer: B (LEAVE A REPLY)
According to the CISM Review Manual (Digital Version), page 5, information security culture is the set of values, attitudes, and behaviors that shape how an organization and its employees view and practice information security. Transforming the information security culture requires a change management process that involves the following steps: creating a sense of urgency, forming a powerful coalition, developing a vision and strategy,

communicating the vision, empowering broad-based action, generating short-term wins, consolidating gains and producing more change, and anchoring new approaches in the culture1. Among the four options, strong management support is the best enabler for transforming the information security culture, as it can provide the necessary leadership, resources, sponsorship, and alignment for the change management process. Periodic compliance audits, robust technical security controls, and incentives for security incident reporting are important elements of information security, but they are not sufficient to change the culture without strong management support. References = 1: CISM Review Manual (Digital Version), page 5

NEW QUESTION: 408
Which of the following parties should be responsible for determining access levels to an application that processes client information?
A. The business client
B. The information security tear
C. The identity and access management team
D. Business unit management
Answer: D (LEAVE A REPLY)
The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.
The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals

and strategies. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

NEW QUESTION: 409
After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?
A. Calculating cost of the incident
B. Conducting a postmortem assessment
C. Performing an impact analysis
D. Preserving the evidence
Answer: (SHOW ANSWER)
The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future.
References = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

NEW QUESTION: 410
To help users apply appropriate controls related to data privacy regulation, what is MOST important to communicate to the users?
A. Data classification policy
B. Features of data protection products
C. Data storage procedures
D. Results of penetration testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 411
Which of the following is the PRIMARY objective of incident triage?
A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats
Answer: C (LEAVE A REPLY)

The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization's information security.
Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization's assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident.
References = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; Critical Incident Stress Management - National Interagency Fire Center3; Critical Incident Stress Management - US Forest Service4

NEW QUESTION: 412
In violation of a policy prohibiting the use of cameras at the office, employees have been issued smartphones and tablet computers with enabled web cameras. Which of the following should be the information security manager's FIRST course of action?
A. Revise the policy.
B. Perform a root cause analysis.
C. Conduct a risk assessment,
D. Communicate the acceptable use policy.
Answer: C (LEAVE A REPLY)
= The information security manager's first course of action in this situation should be to conduct a risk assessment, which is a process of identifying, analyzing, and evaluating the information security risks that arise from the violation of the policy prohibiting the use of cameras at the office. The risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate use of the cameras on the smartphones and tablet computers, such as capturing, transmitting, or disclosing sensitive or confidential information, compromising the privacy or security of the employees, customers, or partners, or violating the legal or regulatory requirements. The risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to disable, restrict, or monitor the camera usage, enforcing the policy compliance and awareness, or revising the policy to reflect the

current business needs and environment. The 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 policy and the risk management process.
Revising the policy, performing a root cause analysis, and communicating the acceptable use policy are all possible courses of action that the information security manager can take after conducting the risk assessment, but they are not the first ones. Revising the policy is a process of updating and modifying the policy to align with the business objectives and strategy, to address the changes and challenges in the business and threat environment, and to incorporate the feedback and suggestions from the risk assessment and the stakeholders.
Performing a root cause analysis is a process of investigating and identifying the underlying causes and factors that led to the violation of the policy, such as the lack of awareness, training, or enforcement, the inconsistency or ambiguity of the policy, or the conflict or gap between the policy and the business requirements or expectations.
Communicating the acceptable use policy is a process of informing and educating the employees and the other users of the smartphones and tablet computers about the purpose, scope, and content of the policy, the roles and responsibilities of the users, the benefits and consequences of complying or violating the policy, and the methods and channels of reporting or resolving any policy issues or incidents. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question
1482

NEW QUESTION: 413
An information security manager is working to incorporate media communication procedures into the security incident communication plan. It would be MOST important to include:
A. a directory of approved local media contacts
B. pre-prepared media statements
C. procedures to contact law enforcement
D. a single point of contact within the organization
Answer: D (LEAVE A REPLY)
A single point of contact within the organization is the most important element to include when incorporating media communication procedures into the security incident communication plan because it helps to ensure a consistent and accurate message to the public and avoid confusion or misinformation. A single point of contact is a designated person who is authorized and trained to communicate with the media on behalf of the organization during a security incident. The single point of contact should coordinate with the incident response team, senior management, legal counsel, and public relations to prepare and deliver timely and appropriate statements to the media, as well as to respond to any inquiries or requests. A single point of contact also helps to prevent unauthorized or

conflicting disclosures from other employees or stakeholders that may harm the organization's reputation or legal position. Therefore, a single point of contact within the organization is the correct answer.
References:
https://www.lifars.com/2020/09/communication-during-incident-response/
https://ifpo.org/resource-links/articles-and-reports/public-and-media-relations/planning-for-effective-media- relations-during-a-critical-incident/
https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan.

NEW QUESTION: 414
Which of the following is the MOST important detail to capture in an organization's risk register?
A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria
D. Risk ownership
Answer: (SHOW ANSWER)
Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

NEW QUESTION: 415
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: A (LEAVE A REPLY)
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: 416
Which of the following should be established FIRST when implementing an information security governance framework?
A. Security architecture
B. Security policies
C. Security incident management team
D. Security awareness training program
Answer: A (LEAVE A REPLY)
This is the most urgent and effective action to prevent further damage or compromise of the organization's network and data. The other options are less important or irrelevant in this situation.
According to How to identify suspicious insider activity using Active Directory, one of the steps to detect and respond to suspicious activity is to isolate the affected device from the network. This can be done by disabling the network adapter, unplugging the network cable, or blocking the device's IP address on the firewall1. This will prevent the device from communicating with any malicious actors or spreading malware to other devices on the network.
`

NEW QUESTION: 417
What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?
A. Vendor service level agreements (SLAs)
B. Independent review of the vendor
C. Local laws and regulations
D. Backup and restoration of data
Answer: C (LEAVE A REPLY)
he greatest concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider is the local laws and regulations that may apply to the data and the cloud service provider. Local laws and regulations may vary significantly across different jurisdictions and may impose different requirements or restrictions on the data protection, privacy, security, sovereignty, retention, disclosure, transfer, or access. These laws and regulations may also create potential conflicts or inconsistencies with the organization's own policies, standards, or contractual obligations.
Therefore, an information security manager should conduct a thorough legal and regulatory analysis before outsourcing data processing to a cloud service provider and

ensure that the cloud service provider complies with all the applicable laws and regulations in the relevant jurisdictions.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Outsourcing2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1
Outsourcing data processing to a cloud service provider may expose the organization to different legal and regulatory requirements depending on the location of the data and the vendor. This could affect the organization's compliance and liability in case of a breach or dispute. Therefore, the information security manager should be most concerned about the local laws and regulations that apply to the outsourcing arrangement.

NEW QUESTION: 418
When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure:
A. the integrity of evidence is preserved.
B. forensic investigation software is loaded on the server.
C. the server is unplugged from power.
D. the incident is reported to senior management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 419
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: 420
An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:
A. risk assessment results.
B. the security organization structure.
C. international security standards.
D. the most stringent requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 421
Which of the following is the BEST indication of an effective information security program?
A. Risk is treated to an acceptable level.
B. The number of security incidents reported by staff has increased.
C. Key risk indicators (KRIs) are established.
D. Policies are reviewed and approved by senior management.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
An effective information security program aims to manage risks to acceptable levels while supporting business objectives.
* A. Risk is treated to an acceptable level: This is the BEST answer as it directly reflects the program's success in mitigating risks within the organization's tolerance levels.
* B. The number of security incidents reported by staff has increased: An increase in reported incidents might indicate improved awareness but does not necessarily reflect overall effectiveness.
* C. Key risk indicators (KRIs) are established: KRIs are important for monitoring risks but do not indicate whether risks are being effectively managed.
* D. Policies are reviewed and approved by senior management: While essential, this action alone does not demonstrate the program's effectiveness.
Reference: CISM Job Practice Area 2 (Risk Management) highlights the importance of risk treatment and its alignment with organizational risk tolerance.

NEW QUESTION: 422
What should be the FIRST step when implementing data loss prevention (DLP) technology?
A. Perform a cost benefit analysis
B. Build a business case
C. Perform due diligence with vendor candidates
D. Classify the organization's data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 423
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: C (LEAVE A REPLY)
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.

NEW QUESTION: 424
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: 425
Which of the following would provide the MOST value to senior management when presenting the results of a risk assessment?
A. Providing a technical risk assessment report
B. Mapping the risks to existing controls
C. Illustrating risk on a heat map
D. Mapping the risks to the security classification scheme
Answer: C (LEAVE A REPLY)

NEW QUESTION: 426
Which of the following is the FIRST step in developing a business continuity plan (BCP)?
A. Determine available resources.
B. Identify critical business processes.
C. Identify the applications with the shortest recovery time objectives (RTOs).
D. Determine the business recovery strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 427
While responding to a high-profile security incident, an information security manager observed several deficiencies in the current incident response plan. When would be the BEST time to update the plan?
A. While responding to the incident
B. During a tabletop exercise
C. During post-incident review
D. After a risk reassessment
Answer: C (LEAVE A REPLY)
During post-incident review is the best time to update the incident response plan after observing several deficiencies in the current plan while responding to a high-profile security incident. A post-incident review is a process of analyzing and evaluating the incident response activities, identifying the lessons learned, and documenting the recommendations and action items for improvement. Updating the incident response plan during post-incident review helps to ensure that the plan reflects the current best practices, addresses the gaps and weaknesses, and incorporates the feedback and suggestions from the incident response team and other stakeholders. Therefore, during post-incident review is the correct answer.
References:
* https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

* https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident- response-plan
* https://www.integrify.com/blog/posts/incident-response-plan-need-an-update/

NEW QUESTION: 428
An organization experienced a loss of revenue during a recent disaster. Which of the following would BEST prepare the organization to recover?
A. Business impact analysis (BIA)
B. Disaster recovery plan (DRP)
C. Incident response plan
D. Business continuity plan (BCP)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 429
Which of the following is MOST important for the information security manager to include when presenting changes in the security risk profile to senior management?
A. Number of false positives
B. Industry benchmarks
C. Security training test results
D. Performance measures for existing controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 430
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: 431
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: 432
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: B (LEAVE A REPLY)

NEW QUESTION: 433
Of the following, whose input is of GREATEST importance in the development of an information security strategy?
A. Process owners
B. End users
C. Security architects.
D. Corporate auditors
Answer: A (LEAVE A REPLY)
Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them.
Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to. Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. References = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

NEW QUESTION: 434

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: 435

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

A. File integrity monitoring software

B. Security information and event management (SIEM) tool

C. Antivirus software

D. Intrusion detection system (IDS)

Answer: (SHOW ANSWER)

An intrusion detection system (IDS) is a software or hardware device that monitors network traffic and detects unauthorized or malicious activities, such as attacks, intrusions, or breaches. An IDS can provide valuable evidence for an information security team to investigate an alleged breach of an organization's network, as it can capture and analyze the network traffic in real time or after the fact. An IDS can help to identify the source, type, scope, and impact of the breach, as well as to generate alerts and reports for further investigation.

File integrity monitoring software (FIM), security information and event management (SIEM) tool, and antivirus software are not single sources of evidence for an information security team to review. FIM software monitors files and directories on a network or system and detects changes or modifications that may indicate unauthorized access or tampering.

SIEM tool collects and correlates data from various sources, such as logs, events, alerts, incidents, and threats, and provides a unified view of the security posture of an organization.
Antivirus software scans files and programs on a network or system and detects malware infections that may compromise the security or functionality of the system.
However, these tools are not sufficient by themselves to provide conclusive evidence for an information security team to investigate an alleged breach of an organization's network. They may provide some clues or indicators of compromise (IOCs), but they may also generate false positives or negatives due to various factors, such as configuration errors, user behavior, benign activities, or evasion techniques. Therefore, an information security team should use multiple sources of evidence from different tools and methods to verify the validity and reliability of the findings.
References = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Evidence Collection1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 436
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?
A. Updated security policies
B. Defined security standards
C. Threat intelligence
D. Regular antivirus updates
Answer: B (LEAVE A REPLY)
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the

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

NEW QUESTION: 437
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: 438
What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?
A. Define the issues to be addressed.
B. Perform a cost-benefit analysis.
C. Calculate the total cost of ownership (TCO).
D. Conduct a feasibility study.
Answer: (SHOW ANSWER)
The first step when developing a business case for a new intrusion detection system (IDS) solution is to define the issues to be addressed. A business case is a document that provides the rationale and justification for initiating a project or investment. It typically includes information such as the problem statement, the objectives, the alternatives, the costs and benefits, the risks and assumptions, and the expected outcomes. The first step in developing a business case is to define the issues to be addressed, which means identifying and describing the current situation, the problems or challenges faced by the organization, and the needs or opportunities for improvement. By defining the issues to be addressed, the information security manager can establish the scope and purpose of the business case, and provide a clear and compelling problem statement that explains why a new IDS solution is needed. The other options are not the first step when developing a business case for a new IDS solution, although they may be part of the subsequent steps. Performing a cost-benefit analysis is a step that involves comparing the costs and benefits of different alternatives, including the new IDS solution and the status quo. A cost-benefit analysis can help evaluate and justify the feasibility and desirability of each alternative, and support the decision-making process. Calculating the total cost of ownership (TCO) is a step that involves estimating the direct and indirect costs associated with acquiring, operating, maintaining, and disposing of an asset or a system over its entire life cycle. A TCO calculation can help determine the long-term financial implications of investing in a new IDS solution, and compare it with other alternatives. Conducting a feasibility study is a step that involves assessing the technical, operational, legal, and economic aspects of implementing a project or an investment. A feasibility study can help identify and mitigate any potential issues or risks that may affect the success of the project or investment, and provide recommendations for improvement

NEW QUESTION: 439
When selecting metrics to monitor the effectiveness of an information security program, it is MOST important for an information security manager to:
A. identify the program's risk and compensating controls.

B. consider the organization's business strategy.
C. consider the strategic objectives of the program.
D. leverage industry benchmarks.
Answer: (SHOW ANSWER)

NEW QUESTION: 440
Which of the following elements of a service contract would BEST enable an organization to monitor the information security risk associated with a cloud service provider?
A. Indemnification clause
B. Breach detection and notification
C. Compliance status reporting
D. Physical access to service provider premises
Answer: (SHOW ANSWER)
Compliance status reporting is the best element of a service contract that would enable an organization to monitor the information security risk associated with a cloud service provider, as it provides the organization with regular and timely information on the cloud service provider's compliance with the agreed-upon security requirements, standards, and regulations. Compliance status reporting also helps the organization to identify any gaps or issues that need to be addressed or resolved, and to verify the effectiveness of the cloud service provider's controls. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 441
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: B (LEAVE A REPLY)
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: 442
The business value of an information asset is derived from:
A. the threat profile.
B. its criticality.
C. the risk assessment.
D. its replacement cost.
Answer: (SHOW ANSWER)
The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability (CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it.
References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

NEW QUESTION: 443
Which of the following is the PRIMARY reason to review the firewall logs when an external network-based attack is reported by the intrusion detection system (IDS)?
A. To validate the payload signature
B. To validate the incident
C. To devise the incident response strategy
D. To review network configurations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 444
Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?
A. Validate the noncompliance
B. Include the noncompliance in the risk register
C. Implement compensating controls to mitigate the noncompliance
D. Report the noncompliance to senior management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 445
Implementing the principle of least privilege PRIMARILY requires the identification of:

A. job duties
B. data owners
C. primary risk factors.
D. authentication controls
Answer: A (LEAVE A REPLY)
Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources. The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.
The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users.
Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege, but they are not the ones who determine the job duties of the users.
References = Principle of least privilege What Is the Principle of Least Privilege and Why is it Important? - F5 1
4

NEW QUESTION: 446
Which of the following metrics would BEST demonstrate the success of a newly implemented information security framework?
A. A decrease in the number of security policy exceptions
B. An increase in the number of compliant business processes
C. An increase in the number of identified security incidents
D. A decrease in the number of security audit findings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 447
Which of the following should be done FIRST after a ransomware incident has been successfully contained?

A. Notify relevant stakeholders.
B. Conduct forensic analysis.
C. Perform lessons learned.
D. Restore impacted systems.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 448
A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?
A. Determine the required security controls for the new solution
B. Review the disaster recovery plans (DRPs) of the providers
C. Obtain audit reports on the service providers' hosting environment
D. Align the roles of the organization's and the service providers' stats.
Answer: A (LEAVE A REPLY)
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 449
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: D (LEAVE A REPLY)
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: 450
An organization is planning to open a new office in another country. Sensitive data will be routinely sent between the two offices. What should be the information security manager's FIRST course of action?
A. Develop customized security training for employees at the new office
B. Encrypt the data for transfer to the head office based on security manager approval
C. Update privacy policies to include the other country's laws and regulations
D. Identify applicable regulatory requirements to establish security policies
Answer: (SHOW ANSWER)
The first course of action is to identify applicable regulatory requirements (D). CISM governance requires understanding legal and regulatory obligations before defining policies, controls, or technical measures.
Encryption (B), training (A), and policy updates (C) must be based on regulatory requirements to ensure compliance and avoid legal exposure. Jurisdictional risk assessment is foundational when operating across borders.
References: ISACA CISM Review Manual (Governance-legal and regulatory compliance); CISM Exam Content Outline (Domain 2).