ISACA.CISM.v2026-09-12.q494

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	494
Version:	v2026-09-12
# of views:	104
# of Questions views:	5052
https://www.freecram.net/torrent/ISACA.CISM.v2026-09-12.q494.html	

NEW QUESTION: 1
Which of the following is MOST likely to be the cause of systems and applications missing critical patches?
A. Insufficient management oversight
B. Inadequate reporting on damaged hardware
C. Lack of a release and deployment policy
D. Outdated configuration management database (CMDB)
Answer: (SHOW ANSWER)
The most likely cause of systems and applications missing critical patches is a lack of a release and deployment policy . CISM program management emphasizes that patching must be governed through formal change, release, and deployment processes to ensure updates are tested, approved, scheduled, deployed, and verified. Without a release and deployment policy, patches may not be consistently prioritized, assigned, implemented, or tracked to completion. Insufficient management oversight can contribute to poor patching, but the more direct cause is the absence of a formal process governing patch release and deployment.
Reporting on damaged hardware is unrelated to missing software patches. An outdated CMDB can cause some assets to be missed, but it does not fully explain missing critical patches across systems and applications as effectively as the lack of a defined deployment policy. CISM stresses that repeatable operational processes are essential to maintain control effectiveness. Therefore, the absence of a release and deployment policy is the best answer.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - patch management and release/deployment controls ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 2

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: 3

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: 4

Which of the following is the MOST important consideration when planning to implement artificial intelligence to enhance an organization's vulnerability and control deficiency analysis capabilities?

A. The alignment of artificial intelligence tools with the organization's existing security policies

B. The adaptability and scalability of artificial intelligence tools

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

NEW QUESTION: 5
The MOST important reason for having an information security manager serve on the change management committee is to:
A. ensure changes are properly documented.
B. advise on change-related risk.
C. ensure that changes are tested.
D. identify changes to the information security policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?
A. Embedding compliance requirements within operational processes
B. Engaging external experts to provide guidance on changes in compliance requirements
C. Performing periodic audits for compliance with legal and regulatory requirements
D. Assigning the operations manager accountability for meeting compliance requirements
Answer: (SHOW ANSWER)
Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing

assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes. Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2. Compliance requirements may vary depending on the industry, location, and nature of the organization2. Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

NEW QUESTION: 7
Which of the following is MOST important to include in monthly information security reports to the board?
A. Trend analysis of security metrics
B. Risk assessment results
C. Root cause analysis of security incidents
D. Threat intelligence
Answer: (SHOW ANSWER)
The most important information to include in monthly information security reports to the board is the trend analysis of security metrics. Security metrics are quantitative and qualitative measures that indicate the performance and effectiveness of the information security program and the alignment with the business objectives. Trend analysis is the process of comparing and evaluating the changes and patterns of security metrics over time. Trend analysis can help to identify the strengths and weaknesses of the information security program, the progress and achievements of the security goals and initiatives, the gaps and opportunities for improvement, and the impact and value of the information security investments. Trend analysis can also help to communicate the current and future security risks and challenges, and the recommended actions and strategies to address them. Trend analysis can provide the board with a clear and concise overview of the information security status and direction, and enable informed and timely decision making.
References =
* CISM Review Manual 15th Edition, page 1631
* The CISO's Guide to Reporting Cybersecurity to the Board2
* CISM 2020: Information Security Metrics and Reporting, video 13

NEW QUESTION: 8
Which of the following is the BEST way to determine the gap between the present and desired state of an information security program?
A. Perform a risk analysis for critical applications.
B. Determine whether critical success factors (CSFs) have been defined.
C. Conduct a capability maturity model evaluation.
D. Review and update current operational procedures.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 9
Which of the following BEST determines an information asset's classification?
A. Value of the information asset in the marketplace
B. Criticality to a business process
C. Risk assessment from the data owner
D. Cost of producing the information asset
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

NEW QUESTION: 10
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:
Freecram.net
A. require that the change be reversed
B. review the change management process
C. perform an analysis of the change
D. report the event to senior management
Answer: (SHOW ANSWER)
Performing an analysis of the change is the first step in addressing the issue of an IT employee making a change to a firewall rule outside of the change control process because it helps to understand the reason, impact, and risk of the change and to decide whether to approve, reject, or reverse it. Requiring that the change be reversed is not the first step because it may cause more disruption or damage without proper analysis and testing. Reviewing the change management process is not the first step because it does not address the specific issue or incident at hand, but rather focuses on improving the process for future changes.

Reporting the event to senior management is not the first step because it does not resolve the issue or incident, but rather escalates it without sufficient information or recommendation.
References: https://www.isaca.org
/resources/isaca-journal/issues/2018/volume-3/change-management-in-the-age-of-digital-transformation
https://www.isaca.org/resources/isaca-journal/issues/

NEW QUESTION: 11
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: (SHOW ANSWER)
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: 12
Which of the following is the MOST important requirement for a successful security program?
A. Mapping security processes to baseline security standards
B. Penetration testing on key systems
C. Management decision on asset value
D. Nondisclosure agreements (NDA) with employees
Answer: C (LEAVE A REPLY)

"A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value."

NEW QUESTION: 13
Which of the following is the MOST effective way to prevent information security incidents?
A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment
Answer: (SHOW ANSWER)
The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management (SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

NEW QUESTION: 14
Which of the following is MOST helpful to identify whether information security policies have been followed?
A. Detective controls
B. Preventive controls
C. Directive controls
D. Corrective controls
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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. Assess the control state.
B. Replace the control.
C. Report the failure to management.
D. Check for defense in depth.
Answer: (SHOW ANSWER)

Upon learning a control is ineffective, the first action should be to assess the state of the control to verify the issue, determine its root cause, and assess the risk exposure. The CISM Review Manual emphasizes that assessment comes before taking further steps like replacement or escalation, as it informs appropriate, risk- based action.
Reference:ISACA CISM Review Manual, 16th Edition, Page 131-132, "Control Assessment and Continuous Improvement".

NEW QUESTION: 16
Which of the following BEST enables an information security manager to demonstrate the effectiveness of the information security and risk program to senior management?
A. Updated risk assessments
B. Counts of information security incidents
C. Monthly metrics
D. Audit reports
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 17
For an enterprise implementing a bring your own device program, which of the following would provide the BEST security for corporate data residing on unsecured mobile devices?
A. Acceptable use policy
B. Containerization solution
C. Data loss prevention
D. Device certification process
Answer: (SHOW ANSWER)
The correct answer is B because containerization separates corporate data and applications from personal data and applications on a mobile device. In a bring your own device environment, the organization does not fully control the endpoint because it is personally owned and may be used on untrusted networks or with unmanaged applications. A containerization solution helps protect enterprise information by enforcing encryption, access controls, remote wipe, data sharing restrictions, and policy controls within the corporate container. An acceptable use policy is important, but it is administrative and does not technically protect data stored on the device. Data loss prevention can help detect or block unauthorized data movement, but it may not provide the

same direct separation and control over mobile data. A device certification process helps assess device suitability, but certification alone does not secure corporate data after deployment. In CISM, controls should be selected based on risk and effectiveness. Containerization is the strongest option for protecting corporate data on unsecured BYOD devices.
Reference: CISM Information Risk Management; mobile device risk, BYOD security, data protection, and compensating control principles.

NEW QUESTION: 18
What is the MOST important consideration for an organization operating in a highly regulated market when new regulatory requirements with high impact to the business need to be implemented?
A. Enforcing strong monitoring controls
B. Conducting a gap analysis
C. Engaging an external audit
D. Establishing compensating controls
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following is the MOST important consideration when briefing executives about the current state of the information security program?
A. Including a situational forecast
B. Using appropriate language for the target audience
C. Including trend charts for metrics
D. Using a rating system to demonstrate program effectiveness
Answer: (SHOW ANSWER)
= When briefing executives about the current state of the information security program, the most important consideration is to use appropriate language for the target audience. This means avoiding technical jargon, acronyms, and details that may confuse or bore the executives, and instead focusing on the business value, risks, and benefits of the information security program. The other options are not as important or relevant as using appropriate language, although they may also be useful to include in the briefing. For example, a situational forecast may be helpful to show the future trends and challenges, but it is not as essential as communicating the current state clearly and concisely. Similarly, trend charts for metrics and a rating system to demonstrate program effectiveness may be useful to support the briefing, but they are not as critical as using language that the executives can understand and relate to. References = Information Security Guide for Government Executives, page 7: "Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment." Information security guide for government executives - NIST, page 3: "The executive should communicate the importance of information security to the organization and its staff, using language that is meaningful to the target audience." Information Security Committee Charter - SecurityStudio,

page 1: "The committee also coordinates and communicates the direction, current state, and oversight of the information security program."

NEW QUESTION: 20

What is the PRIMARY benefit to an organization that maintains an information security governance framework?

Freecram.net

A. Resources are prioritized to maximize return on investment (ROI)

B. Information security guidelines are communicated across the enterprise_

C. The organization remains compliant with regulatory requirements.

D. Business risks are managed to an acceptable level.

Answer: (SHOW ANSWER)

According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.

Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.

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

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

NEW QUESTION: 21

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

A. System owners have been identified.

B. Key applications have been secured.

C. Information assets have been classified.

D. Information assets have been inventoried.

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

NEW QUESTION: 22
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: (SHOW ANSWER)
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: 23
Which of the following is MOST important to the effectiveness of an information security steering committee?
A. The committee has cross-organizational representation.
B. The committee has strong regulatory knowledge.
C. The committee uses a risk management framework.
D. The committee is comprised of representatives from senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 24

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: 25

An organization is MOST likely to accept the risk of noncompliance with a new regulatory requirement when:

A. employees are resistant to the controls required by the new regulation.

B. the regulatory requirement conflicts with business requirements.

C. the risk of noncompliance exceeds the organization's risk appetite.

D. the cost of complying with the regulation exceeds the potential penalties.

Answer: (SHOW ANSWER)

An organization is most likely to accept the risk of noncompliance with a new regulatory requirement when the cost of complying with the regulation exceeds the potential penalties. In

such cases, from a cost-benefit perspective, the organization might find it more economical to absorb potential fines or penalties rather than implementing costly controls or processes to comply with the regulation.
"Risk acceptance occurs when the cost of mitigating or transferring the risk exceeds the benefit of the mitigation. This also applies to regulatory noncompliance if the penalties are less than the costs of compliance."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* ISACA's practice questions highlight that risk acceptance is a legitimate treatment when costs outweigh potential penalties or impact.

NEW QUESTION: 26
Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:
A. perform testing to compare control performance against industry levels.
B. prepare to adapt the controls for future system upgrades.
C. hand over the controls to the relevant business owners.
D. ensure the controls are regularly tested for ongoing effectiveness.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
An organization experienced a loss of revenue during a recent disaster. Which of the following would BEST prepare the organization to recover?
A. Incident response plan
B. Disaster recovery plan (DRP)
C. Business impact analysis (BIA)
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)

NEW QUESTION: 28
What type of control is being implemented when a security information and event management (SIEM) system is installed?
A. Preventive
B. Deterrent
C. Detective
D. Corrective
Answer: (SHOW ANSWER)
A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns

any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing https://www.isaca.org /resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 29
Which of the following BEST helps to ensure a third-party backup site continues to meet the organization's information security standards?
A. Service level agreement (SLA)
B. Memorandum of understanding (MoU)
C. Business continuity plan (BCP)
D. Disaster recovery plan (DRP)
Answer: (SHOW ANSWER)
A Service Level Agreement (SLA) is a legally binding document that defines the performance and compliance expectations for third-party services, including information security requirements. It is the best mechanism to ensure that the third-party backup site meets ongoing security standards. "SLAs should include security, availability, and performance expectations to align third-party services with organizational policies."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Third-Party Relationships*

NEW QUESTION: 30
Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?
Freecram.net
A. To facilitate a qualitative risk assessment following the BIA
B. To increase awareness of information security among key stakeholders
C. To ensure the stakeholders providing input own the related risk
D. To obtain input from as many relevant stakeholders as possible
Answer: (SHOW ANSWER)
The most important reason to conduct interviews as part of the business impact analysis (BIA) process is to obtain input from as many relevant stakeholders as possible. A BIA is a process of identifying and analyzing the potential effects of disruptive events on the organization's critical business functions, processes, and resources. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's continuity planning. Interviews are one of the methods to collect data and information for the BIA, and they involve direct and interactive communication with the stakeholders who are involved in or affected by the business functions, processes, and resources. By conducting interviews, the information security manager can obtain input from as many relevant stakeholders as possible, such as business owners, managers, users, customers, suppliers, regulators, and partners. This can help to ensure that the BIA covers

the full scope and complexity of the organization's business activities, and that the BIA reflects the accurate, current, and comprehensive views and expectations of the stakeholders. Interviews can also help to validate, clarify, and supplement the data and information obtained from other sources, such as surveys, questionnaires, documents, or systems. Interviews can also help to build rapport, trust, and collaboration among the stakeholders, and to increase their awareness, involvement, and commitment to the information security and continuity planning.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Impact Analysis (BIA), pages 178-1801; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 65, page 602.

NEW QUESTION: 31
To help ensure that an information security training program is MOST effective its contents should be
A. focused on information security policy.
B. aligned to business processes
C. based on employees' roles
D. based on recent incidents
Answer: (SHOW ANSWER)
"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

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

NEW QUESTION: 32
Senior management wants to thoroughly test a disaster recovery plan (DRP) for a mission-critical system.
Which of the following would provide the MOST reliable results?
A. Structured walk-through
B. Simulation test
C. Full interruption test
D. Parallel test
Answer: (SHOW ANSWER)

NEW QUESTION: 33
In the context of DevSecOps, which of the following BEST enables the identification of vulnerabilities before software is released?
A. Performing integration testing
B. Testing executable code
C. Automating code review
D. Following secure coding standards
Answer: (SHOW ANSWER)
The correct answer is C because automating code review enables vulnerabilities to be identified continuously and early in the DevSecOps pipeline before software is released. DevSecOps integrates security into development and operations through automation, collaboration, and continuous testing. Automated code review tools, including static application security testing, can scan source code for insecure coding patterns, injection flaws, hardcoded credentials, unsafe libraries, and other weaknesses before deployment. Integration testing is useful for verifying that components work together, but it may not identify many code-level security weaknesses. Testing executable code can help detect vulnerabilities later in the pipeline, but finding flaws after code is compiled or packaged may be less efficient than reviewing source code earlier. Secure coding standards are important, but standards alone do not identify vulnerabilities unless compliance is tested. CISM program management emphasizes embedding security into development processes and using controls that support early risk detection. Therefore, automated code review best enables vulnerability identification before release.
Reference: CISM Information Security Program Development and Management; DevSecOps, secure SDLC, automated security testing, code review, and vulnerability management principles.

NEW QUESTION: 34
Of the following, who is BEST positioned to be accountable for risk acceptance decisions based on risk appetite?
A. Information security manager
B. Chief risk officer (CRO)
C. Information security steering committee
D. Risk owner
Answer: (SHOW ANSWER)
The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.

References = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

NEW QUESTION: 35
An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:
* A bad actor broke into a business-critical FTP server by brute forcing an administrative password
* The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
* The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
* After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail Which of the following could have been prevented by conducting regular incident response testing?
A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data
Answer: (SHOW ANSWER)
Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. References: https://www.isaca.org/resources/isaca-journal/issues/2017
/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 36
Network isolation techniques are immediately implemented after a security breach to:
A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.
Answer: (SHOW ANSWER)

Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. References = CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers & Explanations Database -
12 Month Subscription, Question ID: 1162

NEW QUESTION: 37
Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?
A. Return on investment (ROI)
B. Compliance requirements
C. Target audience
D. Criticality of information
Answer: D (LEAVE A REPLY)
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: 38
Which of the following is a PRIMARY function of an incident response team?
A. To provide a single point of contact for critical incidents
B. To provide effective incident mitigation
C. To provide a risk assessment for zero-day vulnerabilities
D. To provide a business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following is MOST important for an organization to have in place to determine the effectiveness of information security governance?

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

NEW QUESTION: 40
Which of the following should be the NEXT step after a security incident has been reported?
A. Escalation
B. Containment
C. Investigation
D. Recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
Which of the following is MOST appropriate to communicate to senior management regarding information risk?
A. Emerging security technologies
B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress
Answer: B (LEAVE A REPLY)
Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2:
Information Risk Management (IRM) [2022 update]

NEW QUESTION: 42

An organization has just updated its backup capability to a new cloud-based solution. Which of the following tests will MOST effectively verify this change is working as intended?

A. Tabletop testing

B. Black box testing

C. Parallel testing

D. Simulation testing

Answer: (SHOW ANSWER)

NEW QUESTION: 43

An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

A. Red team exercise

B. Black box penetration test

C. Disaster recovery exercise

D. Tabletop exercise

Answer: (SHOW ANSWER)

= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low- cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.

A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and

experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A disaster recovery exercise is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high- risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

NEW QUESTION: 44
Which of the following is the MOST important outcome of a post-incident review?
A. The impact of the incident is reported to senior management.
B. The system affected by the incident is restored to its prior state.
C. The person responsible for the incident is identified.
D. The root cause of the incident is determined.
Answer: (SHOW ANSWER)
Determining the root cause of the incident is essential for preventing or minimizing the recurrence of similar incidents, as well as for identifying and implementing corrective actions to improve the security posture of the organization.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.3

NEW QUESTION: 45
Which of the following BEST enables an organization to continuously assess the information security risk posture?
A. Periodic review of the risk register
B. Degree of senior management support
C. Key risk indicators (KRIs)
D. Compliance with industry regulations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following would BEST mitigate accidental data loss events?
A. Conduct periodic user awareness training.
B. Obtain senior management support for the information security strategy.

C. Conduct a data loss prevention (DLP) audit.
D. Enforce a data hard drive encryption policy.
Answer: (SHOW ANSWER)
Conducting periodic user awareness training is the best way to mitigate accidental data loss events because it can educate the users on the causes, consequences, and prevention of data loss, and increase their awareness of the security policies and procedures of the organization. User awareness training can also help users to identify and report potential data loss incidents, and to adopt good practices such as backing up data, encrypting data, and using secure channels for data transmission and storage.
References: The article Mistakes Happen-Mitigating Unintentional Data Loss from the ISACA Journal 2018 states that "user awareness training is the most effective way to prevent unintentional data loss" and that "user awareness training should include information on the types and sources of data loss, the impact and cost of data loss, the legal and regulatory requirements for data protection, the organization's data security policies and procedures, the roles and responsibilities of users in data security, the best practices and tools for data security, and the reporting and escalation process for data loss incidents" (p. 2)1. The Data Spill Management Guide from the Cyber.gov.au website also states that "user awareness training is an important preventative measure to reduce the likelihood of data spills" and that "user awareness training should cover topics such as data classification, data handling, data storage, data transmission, data disposal, and data spill reporting" (p. 2)

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

NEW QUESTION: 47
Which of the following is MOST important to the successful implementation of an information security program?
A. Adequate security resources are allocated to the program.
B. Key performance indicators (KPIs) are defined.
C. A balanced scorecard is approved by the steering committee.
D. The program is developed using global security standards.
Answer: (SHOW ANSWER)
The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives,

comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.
References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 48
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. web surfing controls
C. packet filtering
D. log monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?
A. The risks are reported to the business unit's senior management
B. The risks are escalated to the IT department for remediation
C. The risks are communicated to the central risk function
D. The risks are entered in the organization's risk register
Answer: D (LEAVE A REPLY)
Recording risks in the risk register ensures visibility, accountability, and tracking. This formal documentation is essential for assigning ownership, determining treatment strategies, and ensuring ongoing governance.
A risk that is not entered into the register may go unaddressed. This step supports structured risk tracking and compliance with governance practices.
"The risk register is the primary tool used to track, prioritize, assign, and monitor risks and their treatment. It forms the basis of a structured risk management program."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Documentation and Communication*

NEW QUESTION: 50
Following a risk assessment, an organization has made the decision to adopt a bring your own device (BYOD) strategy. What should the information security manager do NEXT?
Freecram.net
A. Develop a personal device policy
B. Implement a mobile device management (MDM) solution
C. Develop training specific to BYOD awareness
D. Define control requirements

Answer: (SHOW ANSWER)
Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.
References:
* https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating- effective-policies-and-mitigating
* https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

NEW QUESTION: 51
For which of the following is it MOST important that system administrators be restricted to read-only access?
A. User access log files
B. Administrator user profiles
C. Administrator log files
D. System logging options
Answer: (SHOW ANSWER)
User access log files contain records of user activities and actions on the system, which can be used for auditing, monitoring, and investigating purposes. System administrators should not be able to modify or delete these files to ensure their integrity and availability. References = CISM Review Manual, 16th Edition, Chapter 3, Section 3.3.2.11

NEW QUESTION: 52
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. Refer to industry best practices.
B. Provide security awareness training to customers.
C. Assess business impact against security risk.
D. Quantify the security risk to the business.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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: (SHOW ANSWER)

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: 54

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: 55

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

A. Documenting actions taken in sufficient detail
B. Updating key risk indicators (KRIs)
C. Evaluating the performance of incident response team members
D. Evaluating incident response effectiveness
Answer: (SHOW ANSWER)
An information security post-incident review is a process that aims to identify the root causes, impacts, lessons learned, and improvement actions of a security incident. The highest priority during a post-incident review should be evaluating the effectiveness of the incident response, which means assessing how well the incident response plan, procedures, roles, resources, and communication were executed and aligned with the business objectives and requirements. Evaluating the incident response effectiveness can help to identify the gaps, weaknesses, strengths, and opportunities for improvement in the incident response process and capabilities. Documenting actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are also important activities during a post-incident review, but they are not as critical as evaluating the incident response effectiveness, which can provide a holistic and strategic view of the incident response maturity and value.
References =
* ISACA, CISM Review Manual, 16th Edition, 2020, page 2411
* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2192 During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

NEW QUESTION: 56
Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?
A. Metrics to drive the information security program
B. Information security policies
C. A defined security organizational structure
D. An information security strategy
Answer: (SHOW ANSWER)
An information security strategy is the most important element to have in place as a basis for developing an effective information security program that supports the organization's business goals. An information security strategy is a high-level plan that defines the vision, mission, objectives, scope, and principles of information security for the organization1. It also aligns the information security program with the organization's strategy, culture, risk appetite, and

governance framework2. An information security strategy provides the direction, guidance, and justification for the information security program, and ensures that the program is consistent, coherent, and comprehensive3. An information security strategy also helps to prioritize the information security initiatives, allocate the resources, and measure the performance and value of the information security program4.
The other options are not as important as an information security strategy, because they are either derived from or dependent on the strategy. Metrics are used to drive the information security program, but they need to be based on the strategy and aligned with the goals and objectives of the program. Information security policies are the rules and standards that implement the information security strategy and define the expected behavior and responsibilities of the stakeholders. A defined security organizational structure is the way the information security roles and functions are organized and coordinated within the organization, and it should reflect the strategy and the governance model. References = 1: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 2: CISM Review Manual 15th Edition, Chapter 1, Section 1.2 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 4: CISM Review Manual 15th Edition, Chapter 1, Section 1.4 : CISM Review Manual 15th Edition, Chapter 1, Section 1.5 : CISM Review Manual 15th Edition, Chapter 1, Section 1.6 :
CISM Review Manual 15th Edition, Chapter 1, Section 1.7

NEW QUESTION: 57
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?
A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems
Answer: (SHOW ANSWER)
The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.
The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non- compliance. However, SLAs do not necessarily address the specific

procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties. Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems. However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management. References = 1, 2, 3, 4, 5 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident-management- part-1 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident- management-part-1

NEW QUESTION: 58
An information security manager learns that IT personnel are not adhering to the information security policy because it creates process inefficiencies. What should the information security manager do FIRST?
A. Conduct user awareness training within the IT function.
B. Propose that IT update information security policies and procedures.
C. Determine the risk related to noncompliance with the policy.
D. Request that internal audit conduct a review of the policy development process,
Answer: (SHOW ANSWER)
The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

NEW QUESTION: 59
After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?
A. The service level agreement (SLA) was not met.

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

NEW QUESTION: 60
Which of the following is MOST important when defining how an information security budget should be allocated?
Freecram.net
A. Regulatory compliance standards
B. Information security strategy
C. Information security policy
D. Business impact assessment
Answer: (SHOW ANSWER)
Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are-shaping-up.html
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

NEW QUESTION: 61
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: A (LEAVE A REPLY)
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.

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

NEW QUESTION: 62
An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?
A. Determine which country's information security regulations will be used.
B. Merge the two existing information security programs.
C. Apply the existing information security program to the acquired company.
D. Evaluate the information security laws that apply to the acquired company.
Answer: (SHOW ANSWER)
The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

NEW QUESTION: 63
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: 64
Who is BEST suited to determine how the information in a database should be classified?
A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner
Answer: (SHOW ANSWER)
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements.
Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331

NEW QUESTION: 65
Which of the following should be triggered FIRST when unknown malware has infected an organization's critical system?
A. Incident response plan
B. Disaster recovery plan (DRP)
C. Business continuity plan (BCP)
D. Vulnerability management plan
Answer: (SHOW ANSWER)
The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization' s critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses

on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage.
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: 66
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: 67

An organization has discovered that a server processing real-time visual data could be vulnerable to a lateral movement stage in a ransomware attack. Which of the following controls BEST mitigates this vulnerability?

A. Network segmentation

B. Data loss prevention (DLP)

C. Encryption of data in transit

D. Intrusion detection system (IDS)

Answer: A (LEAVE A REPLY)

Network segmentation is the most effective control to prevent lateral movement. In ransomware attacks, attackers often breach one endpoint and move laterally across the network to reach critical assets.

Segmentation limits this movement by isolating systems into different zones or subnets, thereby reducing the attack surface and preventing unauthorized internal traversal.

DLP and encryption are primarily focused on data protection, not internal network movement.

IDS can detect intrusions but does not prevent movement like segmentation does.

"Network segmentation limits the scope of access for compromised systems and is a key strategy in preventing lateral movement in an attack."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Architecture, Section: Network Security* Real-world example: "In the NotPetya and WannaCry incidents, poor internal segmentation allowed malware to propagate rapidly."

NEW QUESTION: 68

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

A. Update the policies to add controls for protecting the data

B. Encrypt the data to the cloud so that the data is secure

C. Conduct a security assessment on the cloud provider

D. Conduct vulnerability scans on the cloud provider

Answer: (SHOW ANSWER)

The correct answer is C because before migrating a human resources application to the cloud, the information security manager should assess the cloud provider's security capabilities, control environment, compliance posture, data protection practices, incident response process, access management, privacy protections, and contractual commitments. Human resources applications often process sensitive personal and employment information, so third-party and cloud risks must be evaluated before migration. Updating policies may be necessary later, but it does not determine whether the provider can adequately protect the data. Encrypting data is important, but encryption alone does not address all cloud risks such as access control, availability, segregation, monitoring, legal jurisdiction, breach notification, and vendor operations. Conducting vulnerability scans on the cloud provider may not be permitted and would provide only a narrow technical

view. CISM emphasizes due diligence and risk assessment when outsourcing or using third-party services.
Therefore, a security assessment of the cloud provider is the best way to support the migration securely.
Reference: CISM Information Risk Management; cloud risk, third-party assessment, due diligence, data protection, and vendor security principles.

NEW QUESTION: 69
The PRIMARY goal of 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. determine why the incident occurred
D. establish the cost of the incident to the business.
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following has the GREATEST influence on an organization's information security strategy?
A. The organization's risk tolerance
B. The organizational structure
C. Industry security standards
D. Information security awareness
Answer: (SHOW ANSWER)
An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives.
Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.
The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.
An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION: 71
Which of the following is the BEST way to prevent insider threats?
A. Enforce separation of duties and least privilege access.
B. Conduct organization-wide security awareness training.
C. Implement strict security policies and password controls.
D. Implement logging for all access activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?
A. Providing evidence that resources are performing as expected
B. Verifying security costs do not exceed the budget
C. Demonstrating risk is managed at the desired level
D. Confirming the organization complies with security policies
Answer: C (LEAVE A REPLY)
The primary focus of a status report on the information security program to senior management is to demonstrate that the risk to the organization's information assets is managed at the desired level, in alignment with the business objectives and risk appetite. This can be achieved by providing relevant and meaningful metrics, indicators, and trends that show the performance, effectiveness, and value of the information security program, as well as the current and emerging risks and the corresponding mitigation strategies. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 73
Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?
A. Risk assessment results
B. Audit findings
C. Key risk indicators (KRIs)
D. Baseline controls
Answer: (SHOW ANSWER)
Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance.
Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are

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

NEW QUESTION: 74
Which of the following BEST enables an organization to maintain an appropriate security control environment?
A. Alignment to an industry security framework
B. Budgetary support for security
C. Periodic employee security training
D. Monitoring of the threat landscape
Answer: (SHOW ANSWER)
Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

NEW QUESTION: 75
Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?
A. Regulatory requirements are being met.
B. Internal compliance requirements are being met.
C. Risk management objectives are being met.
D. Business needs are being met.
Answer: (SHOW ANSWER)
The primary purpose of business continuity and disaster recovery plans is to ensure that the organization can resume its critical business functions within the stated recovery time objectives (RTOs) after a disruptive event. RTOs are based on the business needs and the impact analysis of each function or process. Therefore, meeting the business needs is the best indicator that the plans are effective. Regulatory requirements, internal compliance requirements, and risk management objectives are important factors that influence the development and testing of the plans, but they are not the ultimate measure of their effectiveness. References = CISM Certified

Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3071; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Imperva, Business Continuity & Disaster Recovery Planning (BCP & DRP)3

NEW QUESTION: 76
Which of the following is BEST used to determine the maturity of an information security program?
A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics
Answer: (SHOW ANSWER)
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes.
Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
References:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security- governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing- information-security

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

NEW QUESTION: 77
The MOST important element in achieving executive commitment to an information security governance program is:
A. a defined security framework.
B. a process improvement model
C. established security strategies.
D. identified business drivers.

Answer: (SHOW ANSWER)

The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

NEW QUESTION: 78

Which of the following is the MOST important reason to consider organizational culture when developing an information security program?

A. It helps expedite approval for the information security budget.

B. Security incidents have an adverse impact on the entire organization.

C. Everyone in the organization is responsible for information security.

D. It helps the organization meet compliance requirements.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 79

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

A. Examine firewall logs to identify the attacker.

B. Evaluate the impact to the business.

C. Implement mitigating controls.

D. Notify the regulatory agency of the incident.

Answer: (SHOW ANSWER)

NEW QUESTION: 80

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.

Freecram.net

Which of the following is the BEST risk treatment option in this situation?

A. Transfer the risk by purchasing insurance.
B. Mitigate the risk by applying anonymization on the data set.
C. Accept the risk, as the benefits exceed the potential consequences.
D. Mitigate the risk by encrypting the customer names in the data set.
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following BEST helps to ensure risk appetite is considered during the risk treatment process?
A. Formalized risk management framework
B. Organization-wide risk awareness and training programs
C. Use of a quantitative risk measurement approach
D. Automated monitoring of key risk indicators (KRIs)
Answer: (SHOW ANSWER)
A formalized risk management framework (A) best ensures that risk appetite and risk tolerance are consistently applied during risk treatment decisions (mitigate, transfer, avoid, accept). In CISM risk management, risk appetite must be translated into decision criteria, escalation thresholds, approval authorities, and consistent evaluation methods-all of which are defined and enforced through a framework. Training and awareness (B) support culture, but they do not guarantee that treatment choices align with appetite in a repeatable, auditable way. Quantitative measurement (C) can improve precision, but even strong numbers can be misused without governance rules that tie outcomes to appetite thresholds and approval requirements.
Automated KRI monitoring (D) helps track risk conditions, but it primarily supports ongoing monitoring, not the structured decision-making needed in treatment selection. A risk framework is the mechanism that institutionalizes appetite into processes, roles, reporting, and acceptance criteria.
References: ISACA CISM Review Manual (Risk management-risk appetite/tolerance, risk response, governance and oversight); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 82
Which of the following is MOST effective in monitoring an organization's existing risk?
A. Periodic updates to risk register
B. Risk management dashboards
C. Security information and event management (SIEM) systems
D. Vulnerability assessment results
Answer: (SHOW ANSWER)
Risk management dashboards are the MOST effective in monitoring an organization's existing risk because they provide a visual and interactive representation of the key risk indicators (KRIs) and metrics that reflect the current risk posture and performance of the organization. Risk management dashboards can help to communicate the risk information to various stakeholders, identify trends and patterns, compare actual results with targets and thresholds, and support

decision making and risk response12. Periodic updates to risk register (A) are important to maintain the accuracy and relevance of the risk information, but they are not the most effective in monitoring the existing risk because they do not provide a real-time or dynamic view of the risk situation. Security information and event management (SIEM) systems are effective in monitoring the security events and incidents that may indicate potential or actual threats to the organization, but they are not the most effective in monitoring the existing risk because they do not provide a comprehensive or holistic view of the risk context and impact. Vulnerability assessment results (D) are effective in monitoring the weaknesses and exposures of the organization's assets and systems, but they are not the most effective in monitoring the existing risk because they do not provide a quantitative or qualitative measure of the risk likelihood and consequence. References = 1: CISM Review Manual 15th Edition, page 316-3171; 2: CISM Domain 2: Information Risk Management (IRM) [2022 update]2

NEW QUESTION: 83
A new risk has been identified in a high availability system. The BEST course of action is to:
A. Perform a cost-benefit analysis for mitigating controls
B. Recommend risk acceptance to the business owner
C. Develop and implement a plan to mitigate the identified risk
D. Evaluate and prioritize the identified risk
Answer: (SHOW ANSWER)
The best first step is to evaluate and prioritize the risk to determine the appropriate treatment strategy before implementing mitigation.
"Once risks are identified, they should be evaluated and prioritized to determine the best response (mitigation, transfer, acceptance, or avoidance)."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*
ISACA practice questions confirm the need for evaluation and prioritization before taking further action.

NEW QUESTION: 84
Which of the following is the BEST way to obtain support for a new organization-wide information security program?
A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.
Answer: (SHOW ANSWER)
= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and

maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by:
Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.
Establishing roles and responsibilities for the security program and ensuring accountability and ownership.
Securing adequate resources and budget for the security program and allocating them appropriately.
Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.
Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.
Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges.
Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.
Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization. An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.
Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication,

confusion, or conflict. However, a RACI chart does not ensure the support or commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders. References = CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112 Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition
- ISACA1
Information Security Strategy: The Key to Success - ISACA2
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

NEW QUESTION: 85
Which of the following would BEST ensure that security is integrated during application development?
A. Employing global security standards during development processes
B. Providing training on secure development practices to programmers
C. Performing application security testing during acceptance testing
D. Introducing security requirements during the initiation phase
Answer: (SHOW ANSWER)
Introducing security requirements during the initiation phase would BEST ensure that security is integrated during application development because it would allow the security objectives and controls to be defined and aligned with the business needs and risk appetite before any design or coding is done. This would also facilitate the security by design approach, which is the most effective method to enhance the security of applications and application development activities1. Introducing security requirements early would also enable the collaboration between security professionals and developers, the identification and specification of security architectures, and the integration and testing of security controls throughout the development life cycle2. Employing global security standards during development processes (A) would help to ensure the consistency and quality of security practices, but it would not necessarily ensure that security is integrated during application development. Providing training on secure development practices to programmers (B) would help to raise the awareness and skills of developers, but it would not ensure that security is integrated during application development. Performing application security testing during acceptance testing would help to verify the security of the application before deployment, but it would not ensure that security is integrated during application development. It would also be too late to identify and remediate any security issues that could have been prevented or mitigated earlier in the development process. References = 1: Five Key

Components of an Application Security Program - ISACA1; 2: CISM Domain - Information Security Program Development | Infosec2

NEW QUESTION: 86
An information security manager has confirmed the organization's cloud provider has unintentionally published some of the organization's business data. Which of the following should be done NEXT?
A. Review the cloud provider's service level agreement (SLA).
B. Identify users associated with the exposed data.
C. Invoke the incident response plan.
D. Initiate the organization's data loss prevention (DLP) processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 87
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: 88
Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?
A. Review the previous risk assessment and countermeasures.
B. Perform a new risk assessment,
C. Evaluate countermeasures to mitigate new risks.
D. Transfer the new risk to a third party.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A risk assessment helps to determine the current level of risk exposure and the adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.
The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options.
References = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

NEW QUESTION: 89
Which of the following is the MOST critical input to developing policies, standards, and procedures to secure information assets?
A. Vulnerability assessment
B. Regulatory requirements
C. Industry best practices
D. Enterprise goals
Answer: (SHOW ANSWER)

Enterprise goals are the most critical input because security policies must align with and support the organization's objectives and mission. Policies that do not align with enterprise goals are less likely to gain management support and may not effectively protect key assets.
"Information security must support enterprise goals and objectives to ensure alignment with the broader business strategy."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Alignment with Business Goals and Objectives ISACA's CISM questions reiterate that alignment with enterprise goals is essential for policy effectiveness.

NEW QUESTION: 90

An organization recently activated its business continuity plan (BCP). Employees were notified during the event, but some did not fully follow the communications plan. What is the BEST way to prevent a recurrence?

Freecram.net

A. Enhance external communication instructions in the BCP
B. Perform tabletop testing with appropriate employees
C. Incentivize employees for following the plan
D. Update the business impact analysis (BIA)
Answer: (SHOW ANSWER)
Tabletop testing with appropriate employees (B) is the best way to prevent recurrence because it reinforces roles, communication paths, and expectations through realistic practice. CISM stresses regular testing and exercises to ensure plans are understood and executable under pressure. Updating the BIA (D) or incentivizing behavior (C) does not address understanding gaps. Enhancing instructions (A) alone is insufficient without practice.
References: ISACA CISM Review Manual (Program management-BCP testing and exercises); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 91
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?

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

NEW QUESTION: 92
A business impact analysis (BIA) BEST enables an organization to establish:
A. Total cost of ownership (TCO).
B. Restoration priorities.
C. Annualized loss expectancy (ALE).
D. Recovery methods.
Answer: (SHOW ANSWER)
A business impact analysis (BIA) best enables an organization to establish restoration priorities (B). In CISM, the primary purpose of a BIA is to identify critical business processes, assess the impact of disruptions over time, and determine which functions must be restored first to minimize business impact. Restoration priorities are derived from factors such as maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs), all of which are key BIA outputs.
Total cost of ownership (A) is a financial analysis concept unrelated to continuity planning. Annualized loss expectancy (C) is an output of quantitative risk analysis, not a BIA. Recovery methods (D) are defined after restoration priorities are established and are part of business continuity and disaster recovery planning. CISM emphasizes that the BIA provides the business-driven foundation upon which recovery strategies and methods are later selected.
By clearly defining restoration priorities, the BIA ensures that continuity planning aligns with business objectives, risk appetite, and operational resilience requirements.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - Business Impact Analysis (BIA) purpose and outcomes ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 93

Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?

A. Alignment with industry benchmarks

B. Results of business impact analyses (BIAs)

C. Possibility of reputational loss due to incidents

D. Availability of security budget

Answer: (SHOW ANSWER)

The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

NEW QUESTION: 94

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: 95
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: (SHOW ANSWER)
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: 96
Which of the following BEST enables an organization to identify and contain security incidents?
A. Risk assessments
B. Threat modeling
C. Continuous monitoring
D. Tabletop exercises
Answer: (SHOW ANSWER)
= Continuous monitoring is the process of collecting, analyzing, and reporting on the security status of an organization's information systems and networks. Continuous monitoring enables an organization to identify and contain security incidents by providing timely and accurate information on the security events, alerts, incidents, and threats that may affect the organization. Continuous monitoring also helps to measure the effectiveness and compliance of the security controls, policies, and procedures that are implemented to protect the organization's information assets. Continuous monitoring can be performed using various tools and methods, such as security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), vulnerability scanners, log analyzers, and audit trails.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.2: Continuous Monitoring2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 3

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98
Which of the following events is MOST likely to require an organization to revisit its information security framework?
A. New services offered by IT
B. Changes to the risk landscape
C. A recent cybersecurity attack
D. A new technology implemented
Answer: (SHOW ANSWER)
Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment. References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

NEW QUESTION: 99
Which of the following is the FIRST step to establishing an effective information security program?
A. Conduct a compliance review.
B. Assign accountability.
C. Perform a business impact analysis (BIA).
D. Create a business case.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the first step to establishing an effective information security program is to create a business case that aligns the program objectives with the organization's goals and strategies. A business case provides the rationale and justification for the information security program and helps to secure the necessary resources and support from senior management and other stakeholders. A business case should include the following elements:
The scope and objectives of the information security program

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

NEW QUESTION: 100

In an organization that has an established social media policy, which of the following is the BEST way to reduce the risk associated with personally identifiable information disclosure?

Freecram.net

A. Delivering regular training to employees about social media usage
B. Monitoring employees' social media usage for confidential content
C. Blocking social media sites on the corporate network
D. Controlling access to personally identifiable information within the organization
Answer: (SHOW ANSWER)
The correct answer is D because the most effective way to reduce disclosure risk is to limit access to personally identifiable information to only those individuals who have a legitimate business need. If employees do not have unnecessary access to PII, the likelihood of accidental or intentional disclosure through social media is reduced at the source. Training is important and supports awareness, but it does not prevent inappropriate access to sensitive information.
Monitoring social media may detect some disclosures after they occur, but it is reactive and may also raise privacy and legal concerns. Blocking social media sites on the corporate network is limited because employees may still use personal devices or external networks.
CISM emphasizes risk-based controls, including access management, data protection, and least privilege.
Since the risk involves disclosure of PII, the best preventive control is restricting and controlling access to that information within the organization.
Reference: CISM Information Risk Management; privacy risk, data protection, access control, and least privilege principles.

NEW QUESTION: 101
The PRIMARY objective of performing a post-incident review is to:
A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.
Answer: (SHOW ANSWER)
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.

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

NEW QUESTION: 102
Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?
A. The capabilities and expertise of the information security team
B. The organization's mission statement and roadmap
C. A prior successful information security strategy
D. The organization's information technology (IT) strategy
Answer: (SHOW ANSWER)
= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security strategy with them. The

information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes.
The capabilities and expertise of the information security team (A) are important factors for the information security manager to consider, but they are not the most useful source of information for developing and implementing an information security strategy. The information security team is responsible for executing and maintaining the information security program and activities, such as risk management, security awareness, incident response, and compliance. The information security manager should assess the capabilities and expertise of the information security team to identify the strengths, weaknesses, opportunities, and threats, and to plan the resource allocation, training, and development of the team. However, the capabilities and expertise of the information security team do not directly inform the information security strategy, which should be driven by the organization's business objectives, risk appetite, and security needs.
A prior successful information security strategy is a possible source of information for the information security manager to refer to, but it is not the most useful one. A prior successful information security strategy is a strategy that has been implemented and evaluated by another organization or a previous information security manager, and has achieved the desired security outcomes and benefits. The information security manager can learn from the best practices, lessons learned, and challenges of a prior successful information security strategy, and apply them to the current organization or situation. However, a prior successful information security strategy may not be relevant, applicable, or suitable for the organization, as it may not reflect the current or future business objectives, risk appetite, and security needs of the organization, or the changing threat landscape and business environment.
The organization's information technology (IT) strategy (D) is also a possible source of information for the information security manager to consult, but it is not the most useful one. The IT strategy is a strategy that defines the IT vision, goals, and initiatives of the organization, and how IT supports and enables the business processes and activities. The information security manager should review the IT strategy to understand the IT infrastructure, systems, and services of the organization, and how they relate to the information security program and activities. However, the IT strategy is not the primary driver of the information security strategy, which should be aligned with the organization's business objectives, risk appetite, and security needs, and not only with the IT objectives, capabilities, and requirements.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy Development, page 23-241

NEW QUESTION: 103
Which of the following activities is MOST appropriate to conduct during the eradication phase of a cyber incident response?
A. Restore affected systems for normal operations.
B. Mitigate exploited vulnerabilities to stop future incidents.

C. Isolate affected systems to prevent further damage
D. Estimate the amount of damage caused by the incident.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which of the following would provide the MOST effective security outcome in an organizations contract management process?
A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage
B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage
C. Extending security assessment to cover asset disposal on contract termination
D. Extending security assessment to include random penetration testing
Answer: (SHOW ANSWER)
Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance. Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

NEW QUESTION: 105
Which of the following will BEST facilitate integrating the information security program into corporate governance?
A. Documentation of the threat landscape
B. An up-to-date security strategy
C. A minimum security baseline
D. Documentation of residual risk
Answer: (SHOW ANSWER)
Documentation of residual risk (D) best facilitates the integration of the information security program into corporate governance because it directly supports executive decision-making and accountability, which are core elements of governance in CISM. Corporate governance requires

senior management and the board to understand, evaluate, and formally accept risk in alignment with business objectives and risk appetite.
Residual risk documentation clearly communicates what risk remains after controls are applied and whether that risk is within acceptable tolerance.
While documentation of the threat landscape (A), an up-to-date security strategy (B), and a minimum security baseline (C) are all important program components, they primarily support operational security management, not governance integration. Governance focuses on oversight, transparency, and risk ownership, all of which are enabled when residual risk is documented, reported, and escalated appropriately.
CISM emphasizes that integrating security into corporate governance requires framing security outcomes in business risk terms that executives can act upon. Residual risk documentation provides the mechanism for informed risk acceptance, prioritization of investments, and alignment with enterprise risk management.
References:
ISACA CISM Review Manual, Information Security Governance - risk reporting, residual risk, and governance integration ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 106
Which of the following provides the MOST comprehensive insight into ongoing threats facing an organization?
A. Business impact analysis (BIA)
B. Risk register
C. Penetration testing
D. Vulnerability assessment
Answer: (SHOW ANSWER)
A risk register is a document that records and tracks the information security risks facing an organization, such as their sources, impacts, likelihoods, responses, and statuses. A risk register provides the most comprehensive insight into ongoing threats facing an organization, as it covers both internal and external threats, as well as their current and potential effects on the organization's assets, processes, and objectives. A risk register also helps to prioritize and monitor the risk mitigation actions and controls, and to communicate the risk information to relevant stakeholders. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a business impact analysis (BIA) is a process that identifies and evaluates the critical business functions, assets, and dependencies of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA does not provide a comprehensive insight into ongoing threats facing an organization, as it focuses more on the consequences of the threats, rather than their sources, likelihoods, or responses. A BIA is mainly used to support the business continuity and disaster recovery planning, rather than the information security risk management.

Option C is not the best answer because penetration testing is a method of simulating a malicious attack on an organization's IT systems or networks, to evaluate their security posture and identify any vulnerabilities or weaknesses that could be exploited by real attackers. Penetration testing does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers a specific scope, target, and scenario, rather than the whole range of threats, sources, and impacts. Penetration testing is mainly used to validate and improve the technical security controls, rather than the information security risk management.
Option D is not the best answer because vulnerability assessment is a process of scanning and analyzing an organization's IT systems or networks, to detect and report any flaws or gaps that could pose a security risk.
Vulnerability assessment does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers the technical aspects of the threats, rather than their business, legal, or regulatory implications. Vulnerability assessment is mainly used to identify and remediate the security weaknesses, rather than the information security risk management. References = CISM Review Manual 15th Edition1, pages 258-259; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 306.
A risk register provides the MOST comprehensive insight into ongoing threats facing an organization. This is because a risk register is a document that records and tracks the identified risks, their likelihood, impact, mitigation strategies, and status. A risk register helps an organization to monitor and manage the threats that could affect its objectives, assets, and operations. A risk register also helps an organization to prioritize its response efforts and allocate its resources accordingly.

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

NEW QUESTION: 107
A KEY consideration in the use of quantitative risk analysis is that it:
A. aligns with best practice for risk analysis of information assets.
B. assigns numeric values to exposures of information assets.
C. applies commonly used labels to information assets.
D. is based on criticality analysis of information assets.
Answer: (SHOW ANSWER)
A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of

occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent way, and to support the decision-making process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

NEW QUESTION: 108
Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?
A. Legal
B. Information security
C. Help desk
D. Human resources (HR)
Answer: (SHOW ANSWER)
Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner." SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process." IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access." Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets.

HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

NEW QUESTION: 109
An organization's information security manager reads on social media that a recently purchased vendor product has been compromised and customer data has been posted online. What should the information security manager do FIRST?
A. Perform a business impact analysis (BIA).
B. Notify local law enforcement agencies of a breach.
C. Activate the incident response program.
D. Validate the risk to the organization.
Answer: (SHOW ANSWER)
The first thing that the information security manager should do after reading about a vendor product compromise on social media is to validate the risk to the organization. This means verifying the source and credibility of the information, determining if the organization uses the affected product, and assessing the potential impact and likelihood of the compromise on the organization's data and systems. Validating the risk to the organization will help the information security manager to decide on the appropriate course of action, such as activating the incident response program, notifying relevant stakeholders, or performing a BIA.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for identifying and assessing the risks associated with the use of third-party products and services" and that "the information security manager should monitor and review the security performance and incidents of third-party products and services on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Validating the risk to the organization is the correct answer because it is the first and most important step to take after reading about a vendor product compromise on social media, as it will help the information security manager to confirm the accuracy and relevance of the information, and to evaluate the potential consequences and probability of the compromise on the organization's data and systems" (p. 63). Additionally, the article Defending Against Software Supply Chain Attacks from the CISA website states that "the first step in responding to a software supply chain attack is to validate the risk to the organization by verifying the source and credibility of the information, determining if the organization uses the affected software, and assessing the potential impact and likelihood of the compromise on the organization's data and systems" (p. 2)

NEW QUESTION: 110
Which of the following is the PRIMARY objective of incident triage?
A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats

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

NEW QUESTION: 111
An employee clicked on a malicious link in an email that resulted in compromising company data. What is the BEST way to mitigate this risk in the future?
A. Conduct phishing awareness training.
B. Implement disciplinary procedures.
C. Establish an acceptable use policy.
D. Assess and update spam filtering rules.
Answer: (SHOW ANSWER)
Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

NEW QUESTION: 112
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: 113

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: 114

Which of the following BEST supports investments in an information security program?

A. Gap analysis results

B. Risk assessment results

C. Business impact analysis (BIA)
D. Business cases
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following should be the PRIMARY objective of the information security incident response process?
A. Conducting incident triage
B. Communicating with internal and external parties
C. Minimizing negative impact to critical operations
D. Classifying incidents
Answer: (SHOW ANSWER)
The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents.
The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.
Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed.
However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate

response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION: 116
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: 117
At what point should risk ownership be assigned?
A. When the risk treatment plan is executed
B. When asset ownership is assigned
C. When the risk is identified
D. When the related vulnerability is identified
Answer: (SHOW ANSWER)
Risk ownership should be assigned when the risk is identified (C). CISM emphasizes early assignment of ownership to ensure accountability for analysis, treatment decisions, and monitoring throughout the risk lifecycle. Waiting until treatment execution (A) delays accountability, while asset ownership (B) or vulnerability identification (D) alone does not ensure ownership of the broader business risk. Early ownership ensures risks are properly evaluated, escalated, and managed in line with risk appetite.
References: ISACA CISM Review Manual (Risk management-risk lifecycle and accountability); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 118
Which of the following is MOST critical when creating an incident response plan?
A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Documenting incident notification and escalation processes
D. Aligning with the risk assessment process
Answer: (SHOW ANSWER)
= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION: 119
Which or the following is MOST important to consider when determining backup frequency?
A. Allowable interruption window
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Maximum tolerable outage (MTO)
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which of the following should be updated FIRST to account for new regulatory requirements that impact current information security controls?
Freecram.net
A. Risk register
B. Business impact analysis (BIA)
C. Information security policy
D. Control matrix
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
Which of the following is a viable containment strategy for a distributed denial of service (DDoS) attack?
A. Block IP addresses used by the attacker
B. Redirect the attacker's traffic
C. Disable firewall ports exploited by the attacker.
D. Power off affected servers
Answer: (SHOW ANSWER)

Redirecting the attacker's traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker's traffic is a technique that involves changing the DNS settings or routing tables to send the attacker's traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker's behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server. Redirecting the attacker's traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker's traffic is the correct answer.
References:
* https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation-strategy
* https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy
* https://www.cloudflare.com/learning/ddos/glossary/sinkholing/.

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

NEW QUESTION: 122
Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?
A. Isolate affected systems to prevent the spread of damage
B. Determine the final root cause of the incident
C. Mitigate exploited vulnerabilities to prevent future incidents
D. Remove all instances of the incident from the network
Answer: (SHOW ANSWER)
The containment phase focuses on limiting the scope of the incident. Isolating affected systems immediately helps prevent propagation and further compromise.
"During the containment phase, isolating compromised systems is a key tactic to minimize further impact and enable safe recovery."
- CISM Review Manual 15th Edition, Chapter 4: Incident Response Life Cycle, Section: Containment Strategies*

NEW QUESTION: 123
An information security manager is updating the organization's incident response plan. Which of the following is the BEST way to validate that the process and procedures provided by IT and business units are complete, accurate, and known by all responsible teams?
A. Review the test objectives with stakeholders.
B. Conduct a data breach incident tabletop exercise.
C. Conduct an incident response plan survey.
D. Review data breach incident triage steps.
Answer: (SHOW ANSWER)
Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.
Reference:ISACA CISM Review Manual, 16th Edition, Page 295, "Testing and Validating Incident Response Plans".

NEW QUESTION: 124
Which of the following is MOST important to include in an information security strategy?
A. Stakeholder requirements
B. Risk register
C. Industry benchmarks
D. Regulatory requirements
Answer: (SHOW ANSWER)
Stakeholder requirements are the most important to include in an information security strategy, as they reflect the business needs, objectives, and expectations of the organization and its key stakeholders. Stakeholder requirements also help to align the information security strategy with the enterprise governance and the organizational culture. Risk register, industry benchmarks, and regulatory requirements are important inputs for the information security strategy, but they are not the most important to include.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Task 1.12

NEW QUESTION: 125
Which of the following is the BEST starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities?
A. Controls analysis
B. Emerging risk review
C. Penetration testing
D. Traffic monitoring
Answer: (SHOW ANSWER)

The best starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities is C. Penetration testing. This is because penetration testing is a method of simulating real-world attacks on a network to evaluate its security posture and identify any weaknesses or gaps that could be exploited by malicious actors. Penetration testing can help the information security manager to assess the effectiveness of the existing controls, prioritize the remediation efforts, and demonstrate compliance with the relevant standards and regulations. Penetration testing can also provide valuable insights into the network architecture, configuration, and behavior, as well as the potential impact and likelihood of different types of attacks.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 50, page 14

NEW QUESTION: 126
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: B (LEAVE A REPLY)
= 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: 127
Unintentional behavior by an employee caused a major data loss incident. Which of the following is the BEST way for the information security manager to prevent recurrence within the organization?
A. Implement compensating controls.
B. Enhance the data loss prevention (DLP) solution.
C. Improve the security awareness training program.
D. Communicate consequences for future instances.
Answer: (SHOW ANSWER)

NEW QUESTION: 128

Which of the following should be the PRIMARY objective for creating a culture of security within an organization?

A. To obtain resources for information security initiatives

B. To prioritize security within the organization

C. To reduce risk to acceptable levels

D. To demonstrate control effectiveness to senior management

Answer: (SHOW ANSWER)

The primary objective of creating a security culture is to reduce risk to acceptable levels (C) by influencing employee behavior and decision-making. CISM stresses that culture is a means to an end-not the end itself.

Prioritization (B), resource acquisition (A), and reporting (D) are outcomes or enablers, but the ultimate purpose is effective risk reduction aligned with business objectives. A strong security culture helps prevent incidents, improves compliance, and strengthens resilience through consistent, risk-aware behavior at all levels of the organization.

References: ISACA CISM Review Manual (Program management-security culture and behavior); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 129

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

A. validate the confidentiality during analysis.

B. reinstate original data when accidental changes occur.

C. validate the integrity during analysis.

D. provide backup in case of media failure.

Answer: (SHOW ANSWER)

The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD-ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital evidence123 References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532: Guide to Computer Forensics and Investigations Fourth Edition, page 4-103:
Forensic disk acquisition over the network, Andrea Fortuna, 2018.

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

NEW QUESTION: 130

An organization is considering using a third party to host sensitive archived data. Which of the following is MOST important to verify before entering into the relationship?

Freecram.net

A. The vendor's data centers are in the same geographic region.

B. The encryption keys are not provisled to the vendor.

C. The vendor's controls are in line with the organization's security standards.

D. Independent audits of the vendor's operations are regularly conducted.

Answer: (SHOW ANSWER)

The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor's controls are in line with the organization's security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.

References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

NEW QUESTION: 131

Which of the following BEST facilitates the reporting of useful information about the effectiveness of the information security program?

A. Risk heat map.

B. Security benchmark report.

C. Security metrics dashboard.

D. Key risk indicators (KRIs).

Answer: (SHOW ANSWER)

A security metrics dashboard is a graphical representation of key performance indicators (KPIs) and key risk indicators (KRIs) that provide useful information about the effectiveness of the information security program.

A security metrics dashboard can help communicate the value and performance of the information security program to senior management and other stakeholders, as well as identify areas for improvement and alignment with business objectives. A security metrics dashboard should be concise, relevant, timely, accurate, and actionable.

References = CISM Review Manual 16th Edition, page 163; CISM Review Questions, Answers & Explanations Manual 9th Edition, page 419.

NEW QUESTION: 132

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. Disable emails for staff responsible for wire transfers.
B. Temporarily suspend wire transfers for the organization.
C. Provide awareness training to staff responsible for wire transfers.
D. Provide awareness training to the CEO for this type of phishing attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
An organization that conducts business globally is planning to utilize a third-party service provider to process payroll information. Which of the following issues poses the GREATEST risk to the organization?
A. The third party does not have an independent assessment of controls available for review.
B. The third party has not provided evidence of compliance with local regulations where data is generated.
C. The third-party contract does not include an indemnity clause for compensation in the event of a breach.
D. The third party's service level agreement (SLA) does not include guarantees of uptime.
Answer: (SHOW ANSWER)
The third party's lack of compliance with local regulations poses the greatest risk to the organization, as it may expose the organization to legal, regulatory, or reputational consequences, such as fines, sanctions, lawsuits, or loss of customer trust. Payroll information is considered sensitive personal data that may be subject to different privacy and security laws depending on the jurisdiction where it is generated, processed, or stored. Therefore, the organization should ensure that the third party adheres to the applicable regulations and standards, and obtains the necessary certifications or attestations to demonstrate compliance.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task
1.22; Ensuring Vendor Compliance and Third-Party Risk Mitigation; How to Manage Access Risk Regarding Third-Party Service Providers

NEW QUESTION: 134
Which of the following would BEST enable a new information security manager to assess the current state of information security governance within the organization?
A. Conducting a business impact analysis (BIA) to understand business priorities
B. Analyzing the integration of information security policies and practices within business processes
C. Performing both quantitative and qualitative risk analyses
D. Interviewing key personnel identified within the governance framework
Answer: (SHOW ANSWER)

Analyzing how security policies and practices are integrated into business processes (B) provides the clearest view of governance effectiveness. CISM defines governance as the alignment of security with business objectives, supported by defined roles, accountability, and decision-making structures. BIAs (A) and risk analyses (C) provide valuable inputs but do not directly assess governance maturity. Interviews (D) can supplement understanding but are subjective without observing real integration. By evaluating whether security is embedded in procurement, development, operations, and decision workflows, a new security manager can determine whether governance is formalized, consistently applied, and supported by management.
References: ISACA CISM Review Manual (Governance-structure, integration, and effectiveness); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 135
The PRIMARY reason to properly classify information assets is to determine:
A. the appropriate protection based on sensitivity.
B. appropriate encryption strength using a risk-based approach.
C. the business impact if assets are compromised.
D. user access levels based on the need to know.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?
A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.
Answer: (SHOW ANSWER)
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

Valid CISM Dumps shared by EduDump.com for Helping Passing CISM Exam!
EduDump.com now offer the **newest CISM exam dumps**, the EduDump.com CISM exam

questions have been updated and **answers have been corrected** get the **newest** EduDump.com CISM dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM/premium/ (**1193** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137
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: 138
When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?
A. Recommendations from senior management
B. Business impact analysis (BIA) results
C. The business continuity plan (BCP)
D. Vulnerability assessment results
Answer: (SHOW ANSWER)

NEW QUESTION: 139

How would the information security program BEST support the adoption of emerging technologies?

A. Conducting a control assessment

B. Developing an emerging technology roadmap

C. Providing effective risk governance

D. Developing an acceptable use policy

Answer: (SHOW ANSWER)

An emerging technology roadmap is a strategic plan that identifies the potential benefits, risks, and challenges of adopting new technologies in alignment with the organization's goals and objectives. It also defines the roles and responsibilities, processes, and controls for managing the technology lifecycle, from evaluation to implementation to maintenance. An emerging technology roadmap can help the information security program support the adoption of emerging technologies by ensuring that security requirements are considered and addressed at every stage, and that the technologies are aligned with the organization's risk appetite and compliance obligations.

References = CISM Review Manual, 15th Edition, page 97; Privacy, Security and Bias in Emerging Technologies; The Impact of Emerging Technology on the Future of Cybersecurity

NEW QUESTION: 140

Which of the following would be MOST important to include in a proposal justifying investments for an organization's information security program?

Freecram.net

A. Vulnerability scan results

B. Competitor benchmark analysis

C. Previous security budget

D. Business requirements

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

Justifying investments in information security requires aligning proposals with business objectives to gain management approval.

A). Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.

B). Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.

C). Previous security budget: Historical data may provide context but does not justify future needs.

D). Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders.

Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

NEW QUESTION: 141

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

NEW QUESTION: 142
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: 143

An organization is in the process of selecting a third party to process customer information. Which of the following provides the BEST evidence that the third party's controls will operate as required?

A. Results of incident response tests

B. An independent assessment

C. An external vulnerability assessment

D. An information security questionnaire

Answer: B (LEAVE A REPLY)

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

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

NEW QUESTION: 144

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

A. Frequent incident response training sessions

B. Centralized control monitoring capabilities

C. Responsibilities defined within role descriptions

D. Predetermined service level agreements (SLAs)

Answer: (SHOW ANSWER)

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

Centralized control monitoring capabilities are not very effective because they do not address the communication needs or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or

challenges during an actual incident. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident- response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident- response-lessons-learned

NEW QUESTION: 145
Which of the following is the MOST effective way to help assure the integrity of an organization's accounting system?
A. Providing security awareness training to accounting staff
B. Implementing two-factor authentication
C. Performing frequent security reviews of the audit log
D. Conducting an annual security audit of the system
Answer: C (LEAVE A REPLY)
Frequent security reviews of the audit log (C) most directly assure the integrity of an accounting system by enabling detection of unauthorized or inappropriate transactions and configuration changes. Integrity focuses on accuracy, completeness, and protection from unauthorized modification, and audit logs provide evidence of system activity that can be reviewed for anomalies, fraud, or policy violations. Awareness training (A) is preventive but indirect. Two-factor authentication (B) strengthens access control, but does not detect improper changes made by authorized users. Annual audits (D) are periodic and retrospective, making them less effective for ongoing integrity assurance. CISM emphasizes that detective controls, such as log monitoring and review, are critical for high-integrity systems like financial and accounting applications where timely detection is essential.
References: ISACA CISM Review Manual (Program management-control types, monitoring, integrity assurance); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 146
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: 147
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?
A. Communicate disciplinary processes for policy violations.
B. Require staff to participate in information security awareness training.
C. Require staff to sign confidentiality agreements.
D. Include information security responsibilities in job descriptions.
Answer: (SHOW ANSWER)
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION: 148
Which of the following is MOST difficult to measure following an information security breach?
A. Reputational damage
B. Human resource costs
C. Regulatory sanctions
D. Replacement efforts
Answer: (SHOW ANSWER)
Reputational damage is often intangible, subjective, and hard to quantify, making it the most challenging aspect to measure.

"Reputation impact is difficult to quantify and may have long-term effects that are not immediately apparent."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis* ISACA practice questions highlight that reputational damage is uniquely challenging to measure accurately.

NEW QUESTION: 149
Which of the following is MOST effective for communicating forward-looking trends within security reporting?
A. Key control indicator (KCIs)
B. Key risk indicators (KRIs)
C. Key performance indicators (KPIs)
D. Key goal indicators (KGIs)
Answer: (SHOW ANSWER)
= Security reporting is the process of providing relevant and timely information on the status and performance of the information security program to the stakeholders. Security reporting should be aligned with the business objectives and risk appetite of the organization, and should provide meaningful insights and recommendations for decision making and improvement. Security reporting should also include forward- looking trends, which are projections or predictions of future events or conditions based on historical data, current situation, and external factors. Forward-looking trends can help the organization anticipate and prepare for potential risks and opportunities, and adjust their strategies and plans accordingly.
One of the most effective ways to communicate forward-looking trends within security reporting is to use key risk indicators (KRIs). KRIs are metrics that measure the level of exposure or likelihood of a risk event occurring, and provide early warning signals of potential changes in the risk profile. KRIs can help the organization monitor and manage the key risks that may affect the achievement of their objectives, and take proactive actions to mitigate or avoid them. KRIs can also help the organization identify emerging risks and trends, and evaluate the effectiveness of their risk treatment options. KRIs should be aligned with the risk appetite and tolerance of the organization, and should be regularly reviewed and updated to reflect the changing risk environment.
The other options are not the most effective ways to communicate forward-looking trends within security reporting. Key control indicators (KCIs) are metrics that measure the effectiveness and efficiency of the security controls implemented to reduce the impact or likelihood of a risk event. KCIs can help the organization assess and improve the performance of their security processes and activities, and ensure compliance with the security policies and standards. However, KCIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key performance indicators (KPIs) are metrics that measure the achievement of the security objectives and goals, and demonstrate the value and contribution of the information security program to the organization. KPIs can help the organization evaluate and communicate the results and outcomes of their security initiatives and

projects, and align them with the business strategy and vision. However, KPIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key goal indicators (KGIs) are metrics that measure the progress and completion of the security goals and targets, and indicate the degree of success and satisfaction of the information security program. KGIs can help the organization track and report the status and milestones of their security plans and actions, and ensure alignment with the stakeholder expectations and requirements.
However, KGIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 77-78, 81-821; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 4: Information Security Program Resources, ISACA2

NEW QUESTION: 150

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?

Freecram.net

A. Vendor service level agreements (SLAs)
B. Independent review of the vendor
C. Local laws and regulations
D. Backup and restoration of data
Answer: (SHOW ANSWER)
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: 151
Which of the following BEST determines the data retention strategy and subsequent policy for an organization?
A. Supplier requirements
B. Business impact analysis (BIA)
C. Risk appetite
D. Business requirements
Answer: (SHOW ANSWER)

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

NEW QUESTION: 152
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. Periodic information security training for end users
B. Use of integrated patch deployment tools
C. Regular review of the threat landscape
D. Monitoring of anomalies in system behavior
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Which of the following is the PRIMARY reason to conduct a post-incident review?
A. To notify regulatory authorities
B. To improve the response process
C. To aid in future risk assessments
D. To determine whether digital evidence is admissible
Answer: (SHOW ANSWER)

NEW QUESTION: 154
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 prevent evidence from being disclosed to any internal staff members
B. To provide the response team with expert training on evidence handling
C. To validate the incident response process

D. To ensure evidence is handled by qualified resources
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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: 156
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: 157
Which of the following is the BEST justification for making a revision to a password policy?
A. Vendor recommendation
B. Audit recommendation
C. A risk assessment
D. Industry best practice
Answer: (SHOW ANSWER)
The best justification for making a revision to a password policy is a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a risk assessment, the organization can determine the appropriate level of security controls and measures to protect its information assets and systems, including password policies. A risk assessment can also help identify any gaps or weaknesses in the existing password policy, and provide recommendations for improvement based on the organization's risk appetite and tolerance. The other options are not the best justification for making a revision to a password policy, although they may be some inputs or outputs of the risk assessment process. A vendor recommendation is an external source of advice or guidance that may or may not be relevant or applicable to the organization's specific context and needs. A

vendor recommendation should not be followed blindly without conducting a risk assessment to evaluate its suitability and effectiveness. An audit recommendation is an internal source of feedback or suggestion that may or may not be accurate or complete.
An audit recommendation should not be implemented without conducting a risk assessment to verify its validity and feasibility. An industry best practice is a general standard or guideline that may or may not reflect the organization's unique characteristics and requirements. An industry best practice should not be adopted without conducting a risk assessment to customize it according to the organization's goals and priorities

NEW QUESTION: 158
Data classification is PRIMARILY the responsibility of:
A. senior management.
B. the security manager.
C. the data custodian.
D. the data owner.
Answer: (SHOW ANSWER)

NEW QUESTION: 159
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: 160
Which of the following has The GREATEST positive impact on The ability to execute a disaster recovery plan (DRP)?
Freecram.net
A. Storing the plan at an offsite location
B. Communicating the plan to all stakeholders
C. Updating the plan periodically

D. Conducting a walk-through of the plan

Answer: (SHOW ANSWER)

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

NEW QUESTION: 161

After updating password standards, an information security manager is alerted by various application administrators that the applications they support are incapable of enforcing these standards. The information security manager's FIRST course of action should be to:

A. implement compensating controls.

B. determine the potential impact.

C. evaluate the cost of replacing the applications.

D. reevaluate the standards.

Answer: (SHOW ANSWER)

NEW QUESTION: 162

Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?

A. Residual risk

B. Regulatory requirements

C. Risk tolerance

D. Control objectives

Answer: (SHOW ANSWER)

The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance. References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 163

Which of the following should be the FIRST consideration for an information security manager after a security incident has been confirmed?

A. Executing containment procedures

B. Determining the root cause
C. Developing incident reporting criteria
D. Restoring business operations
Answer: (SHOW ANSWER)
Once a security incident has been confirmed, the first consideration for the information security manager is executing containment procedures (A). According to CISM incident management principles, containment is prioritized immediately after confirmation to limit the spread of the incident, prevent further damage, and protect unaffected systems and data. Delaying containment increases potential impact, data loss, and operational disruption.
Determining the root cause (B) is an important activity but occurs after containment, once the situation is stabilized. Developing incident reporting criteria (C) is part of incident response planning and should already be defined before an incident occurs. Restoring business operations (D) is a recovery-phase activity that follows containment and eradication.
CISM emphasizes a structured incident response lifecycle: confirmation # containment # eradication # recovery # post-incident review. Immediate containment ensures the organization retains control of the incident while preserving evidence and enabling informed decisions for subsequent steps.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident response lifecycle and containment ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 164
Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?
A. Review compliance requirements.
B. Communicate the exposure.
C. Declare an incident.
D. Change the encryption keys.
Answer: (SHOW ANSWER)
Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task
4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

NEW QUESTION: 165
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: 166
During an information security audit, it was determined that IT staff did not follow the established standard when configuring and managing IT systems. Which of the following is the BEST way to prevent future occurrences?
A. Providing annual information security awareness training
B. Conducting periodic vulnerability scanning
C. Implementing a strict change control process
D. Updating configuration baselines
Answer: (SHOW ANSWER)
A strict change control process (C) is the most effective preventive measure because it embeds compliance with standards into the system lifecycle and operational workflow. If staff are deviating from configuration
/management standards, the core issue is often lack of enforced process controls: undocumented changes, rushed fixes, inconsistent approvals, or missing validation. Formal change management ensures changes are requested, risk-assessed, approved by authorized parties, tested, implemented, and reviewed, with traceability and accountability. Annual awareness training (A)

helps general understanding but is weaker than a control that prevents and detects unauthorized deviations. Vulnerability scanning (B) is detective and may identify weaknesses after the fact, but it does not ensure standards are followed. Updating configuration baselines (D) is valuable, but without change control, baselines can still be bypassed. In CISM program management, the best answer typically emphasizes repeatable, auditable processes that reduce human error and enforce governance.
References: ISACA CISM Review Manual (Program management-control implementation, change control governance, assurance and compliance); CISM Exam Content Outline (Domain 3).

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

NEW QUESTION: 167
When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?
A. Data is encrypted in transit and at rest at the vendor site.
B. Data is subject to regular access log review.
C. The vendor must be able to amend data.
D. The vendor must agree to the organization's information security policy,
Answer: (SHOW ANSWER)
When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization's information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization's information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization's right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

NEW QUESTION: 168
An information security manager is considering options for protecting the data on a web-facing legacy application that cannot be patched. Which of the following would provide the BEST information about the effectiveness of compensating controls?
A. Threat assessment
B. Intrusion detection system logs
C. Penetration testing
D. Firewall rules
Answer: C (LEAVE A REPLY)
The correct answer is C because penetration testing provides practical evidence of whether compensating controls can resist real-world attack techniques against the legacy application. When an application cannot be patched, compensating controls such as web application firewalls, network segmentation, access restrictions, monitoring, or virtual patching may be used to reduce risk. However, the effectiveness of those controls should be validated through testing that simulates attacker behavior. A threat assessment identifies potential threats, but it does not prove whether controls are working. Intrusion detection system logs may show detected activity, but they provide only a partial and reactive view. Firewall rules can be reviewed, but rule review alone does not demonstrate whether the total control environment prevents exploitation. Penetration testing is more useful because it tests the application and compensating controls together under realistic conditions. CISM emphasizes risk-based control validation, especially where vulnerabilities cannot be remediated directly. Therefore, penetration testing provides the best information about compensating control effectiveness.
Reference: CISM Information Risk Management; compensating controls, vulnerability management, penetration testing, and control effectiveness principles.

NEW QUESTION: 169
Which of the following would BEST justify continued investment in an information security program?
A. Reduction in residual risk
B. Security framework alignment
C. Speed of implementation
D. Industry peer benchmarking
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. References = CISM Review Manual, 16th Edition, page 431; CISM

Review Questions, Answers & Explanations Manual, 10th Edition, page 622 Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

NEW QUESTION: 170

Which of the following is the MOST common cause of cybersecurity breaches?

A. Lack of adequate password rotation

B. Human error

C. Abuse of privileged accounts

D. Lack of control baselines

Answer: (SHOW ANSWER)

Human error remains the leading cause of cybersecurity breaches, including mishandling data, misconfigurations, and falling for phishing attacks.

"Human error continues to be one of the most common causes of data breaches and security incidents."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Root Cause Analysis*

NEW QUESTION: 171

An information security manager is MOST likely to obtain approval for a new security project when the business case provides evidence of:

A. organizational alignment

B. IT strategy alignment

C. threats to the organization

D. existing control costs

Answer: (SHOW ANSWER)

A new security project is more likely to be approved if it aligns with the organization's goals, objectives, and strategies. This shows that the project supports the business needs and adds value to the organization. Organizational alignment is one of the key elements of a business case for information security, as stated in the CISM Review Manual, 16th Edition1, page 41. IT strategy alignment, threats to the organization, and existing control costs are also important factors to consider, but they are not as persuasive as organizational alignment in obtaining approval for a new security project. References = 1: CISM Review Manual, 16th Edition by Isaca (Author) Learn more:

1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 172

Which of the following is MOST important in order to obtain senior leadership support when presenting an information security strategy?

A. The strategy aligns with management's acceptable level of risk.
B. The strategy addresses ineffective information security controls.
C. The strategy aligns with industry benchmarks and standards.
D. The strategy addresses organizational maturity and the threat environment.
Answer: (SHOW ANSWER)
The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat environment is not a very important factor because it does not indicate how the strategy will advance or adapt the organization's security posture or resilience. 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: 173
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. Understand the cost of noncompliance.
C. Implement a program of work to comply with the new legislation.
D. Consult with senior management on the best course of action.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
In a call center, the BEST reason to conduct a social engineering is to:
A. Identify candidates for additional security training.
B. minimize the likelihood of successful attacks.
C. gain funding for information security initiatives.
D. improve password policy.
Answer: (SHOW ANSWER)
The best reason to conduct a social engineering test in a call center is to identify candidates for additional security training because it helps to assess the level of awareness and skills of the call

center staff in recognizing and resisting social engineering attacks, and provide them with the necessary training or education to improve their security posture. Minimizing the likelihood of successful attacks is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Gaining funding for information security initiatives is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Improving password policy is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. 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: 175
Which of the following is the BEST method for determining whether new risks exist in legacy systems?
A. Regularly scheduled risk assessments
B. Regularly scheduled security audits
C. Frequent updates to the risk register
D. Frequent security architecture reviews
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176
Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?
A. Projected Increase in maturity level
B. Estimated reduction in risk
C. Projected costs over time
D. Estimated increase in efficiency
Answer: (SHOW ANSWER)
The best thing to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its cost-effectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and

processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

NEW QUESTION: 177
Which of the following is the PRIMARY benefit of training service desk staff to recognize incidents?
A. Incident response plan can be activated in a timely manner.
B. Incident metrics can be communicated.
C. Risk response options can be identified quickly.
D. Incident classification times can be improved.
Answer: (SHOW ANSWER)
The service desk is often the first point of contact for users. If trained properly, they can quickly recognize signs of an incident and escalate it, triggering the incident response process promptly. This early detection and escalation are essential for minimizing damage and response time.
"Training frontline support staff ensures timely detection and escalation of incidents, which is critical for effective containment."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Roles and Responsibilities*

NEW QUESTION: 178
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: (SHOW ANSWER)
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: 179

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: 180

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?

Freecram.net

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: 181

Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

A. Revisit the business objective.
B. Escalate to senior management.
C. Perform a cost-benefit analysis.
D. Recommend risk acceptance.
Answer: (SHOW ANSWER)
Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps2. However, this answer is not certain, and you might need to consider other factors as well.

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

NEW QUESTION: 182
When developing an incident escalation process, the BEST approach is to classify incidents based on:
A. estimated time to recover.
B. information assets affected.
C. recovery point objectives (RPOs).
D. their root causes.
Answer: (SHOW ANSWER)
The best approach to developing an incident escalation process is to classify incidents based on the information assets affected, because this will help to determine the impact and severity of the incidents, as well as the appropriate response and recovery actions. The information assets affected by an incident can indicate the potential loss of confidentiality, integrity, or availability of the information, as well as the legal, regulatory, contractual, or reputational implications. By classifying incidents based on the information assets affected, the organization can prioritize the incidents and escalate them to the relevant stakeholders and authorities.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

NEW QUESTION: 183
To ensure the information security of outsourced IT services, which of the following is the MOST critical due diligence activity?
A. Review samples of service level reports from the service provider.

B. Review a recent independent audit report of the service provider.
C. Assess the level of security awareness of the service provider.
D. Request the service provider comply with information security policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 184
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: 185
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: 186
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).
Answer: (SHOW ANSWER)
Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.
Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been

identified and implemented. References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

NEW QUESTION: 187
Which of the following is the MOST effective way to influence organizational culture to align with security guidelines?
A. Adhere to regulatory requirements
B. Conduct security awareness
C. Document and distribute security procedures
D. Communicate and enforce security policies
Answer: (SHOW ANSWER)
Communicating and enforcing policies demonstrates leadership commitment and drives behavior across the organization, fostering a culture of security.
"Policies must be effectively communicated and enforced to influence culture and employee behavior."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Security Culture*

NEW QUESTION: 188
Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?
A. Evaluate privacy technologies required for data protection.
B. Encrypt all personal data stored on systems and networks.
C. Update disciplinary processes to address privacy violations.
D. Create an inventory of systems where personal data is stored.
Answer: (SHOW ANSWER)
= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:
Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.
Assess the risks and impacts associated with the personal data, and the compliance requirements and obligations under the applicable data privacy regulations.

Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.
Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.
Monitor and review the performance and effectiveness of the data protection program, and report and resolve any data breaches or incidents.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Data Protection, pages 202-2051; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 71, page 662.

NEW QUESTION: 189
Which of the following BEST indicates senior management support for an information security program?
A. Top-down communication
B. Regular security awareness training
C. Steering committee involvement
D. Participation in a certification program
Answer: (SHOW ANSWER)
The correct answer is C because active involvement in an information security steering committee demonstrates senior management's ongoing participation in governance, prioritization, decision-making, and oversight. Senior management support is not shown only by words or occasional communication; it is demonstrated through active engagement, resource allocation, risk decisions, and accountability. Top-down communication is useful and may show support, but it is less meaningful than direct participation in a governance body. Regular security awareness training is important for employees, but it does not necessarily prove senior management support. Participation in a certification program may improve professional skills or demonstrate individual commitment, but it is not the best indicator of organizational leadership support. In CISM, information security governance requires senior management direction and oversight to ensure that security objectives align with business objectives. A steering committee provides a formal mechanism for that oversight and involvement. Therefore, steering committee involvement is the best indicator of senior management support.
Reference: CISM Information Security Governance; senior management commitment, steering committee oversight, and governance accountability principles.

NEW QUESTION: 190
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?
Freecram.net
A. Control owner responses based on a root cause analysis

B. The impact of noncompliance on the organization's risk profile
C. A noncompliance report to initiate remediation activities
D. A business case for transferring the risk
Answer: (SHOW ANSWER)
The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions.
Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process." CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

NEW QUESTION: 191
Which of the following should be done FIRST when establishing an information security governance framework?
A. Conduct a cost-benefit analysis of the framework.
B. Gain an understanding of the business and cultural attributes.
C. Contract a third party to conduct an independent review of the program.
D. Evaluate information security tools and skills relevant for the environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 192
Which of the following is the BEST indicator of a successful intrusion into an organization's systems?
A. Increase in the number of irregular application requests
B. Decrease in available storage space
C. Decrease in internal network traffic
D. Increase in the number of failed login attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 193
Which of the following trends would be of GREATEST concern when reviewing the performance of an organization's intrusion detection systems (IDSs)?
A. Decrease in false positives
B. Increase in false positives

C. Increase in false negatives
D. Decrease in false negatives
Answer: (SHOW ANSWER)
An increase in false negatives would be of greatest concern when reviewing the performance of an organization's IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore, a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives.
References = CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

NEW QUESTION: 194
What is the PRIMARY role of the information security program?
A. To perform periodic risk assessments and business impact analyses (BIAs)
B. To provide guidance in managing organizational security risk
C. To approve information security requirements related to the business
D. To educate stakeholders regarding information security requirements
Answer: (SHOW ANSWER)
The primary role of the information security program is to provide guidance in managing organizational security risk (B). In CISM, the security program translates governance direction, policies, and risk appetite into coordinated activities, controls, and practices that enable the organization to manage risk consistently and effectively. Performing risk assessments and BIAs (A) are important activities but are not the program's primary purpose. Approving security requirements (C) is typically a management or governance responsibility, while education and awareness (D) are supporting components of the program. CISM emphasizes that the security program acts as the mechanism for operationalizing risk management, ensuring alignment with business objectives and continuous improvement of the security posture.
References: ISACA CISM Review Manual (Program development and management-program purpose and scope); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 195
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?
A. Monitor the effectiveness of controls
B. Update the risk assessment framework
C. Review the inherent risk level
D. Review the risk probability and impact
Answer: (SHOW ANSWER)

If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

NEW QUESTION: 196
Which of the following is an input used to calculate system-level risk?
A. Key risk indicators
B. Business impact analysis
C. System risk appetite
D. System vulnerabilities
Answer: D (LEAVE A REPLY)
The correct answer is D because system-level risk is calculated or assessed by considering threats, vulnerabilities, likelihood, impact, and existing controls related to a specific system. Vulnerabilities are weaknesses that may be exploited by threats and are therefore direct inputs into determining risk. Key risk indicators are useful for monitoring changes in risk exposure over time, but they are generally reporting or monitoring measures rather than primary calculation inputs. A business impact analysis helps determine the effect of disruption on business processes and may support impact evaluation, but it is not by itself a system- level risk input. System risk appetite defines how much risk may be acceptable, but it does not calculate the risk itself; it is used to evaluate whether calculated or assessed risk is acceptable. In CISM risk management, risk assessment requires identifying assets, threats, vulnerabilities, likelihood, impact, and controls. Since vulnerabilities directly influence the likelihood and potential success of exploitation, system vulnerabilities are the best answer.
Reference: CISM Information Risk Management; risk assessment, vulnerabilities, likelihood, impact, system- level risk, and control evaluation principles.

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

NEW QUESTION: 197

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

A. Perform a gap analysis.

B. Conduct benchmarking.

C. Notify the legal department.

D. Determine the disruption to the business.

Answer: (SHOW ANSWER)

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

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

1. isaca.org2. csoonline.com

NEW QUESTION: 198

Which of the following is MOST important for an information security manager to consider when reviewing a security investment plan?

A. The plan focuses on meeting industry best practices and industry standards.

B. The plan has summarized IT costs for implementation.

C. The plan is based on a review of threats and vulnerabilities.

D. The plan resolves all potential threats to business processes.

Answer: (SHOW ANSWER)

NEW QUESTION: 199

Which of the following activities MUST be performed by an information security manager for change requests?

A. Review change in business requirements for information security.

B. Perform penetration testing on affected systems.

C. Assess impact on information security risk.

D. Scan IT systems for operating system vulnerabilities.

Answer: (SHOW ANSWER)

NEW QUESTION: 200

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

Freecram.net

A. Collect additional metrics.

B. Perform a cost-benefit analysis.

C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.
Answer: (SHOW ANSWER)
The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:
Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

NEW QUESTION: 201
A serious vulnerability was detected in a business application that can be exploited by external attackers to compromise the system. What is the information security manager's BEST course of action?
A. Ask the business application owner to apply the fix immediately
B. Implement temporary remediation
C. Immediately shut down the application
D. Report the risk to the business application owner
Answer: (SHOW ANSWER)
The best course of action is to implement temporary remediation (B) to reduce exposure while a permanent fix is planned and approved. CISM emphasizes balancing risk reduction with business continuity. Immediate shutdown (C) or unilateral action (A) may disrupt business operations without proper authorization. Reporting the risk (D) is necessary but insufficient on its own.

Temporary controls, such as access restrictions or additional monitoring, reduce risk while enabling informed decision-making by the business owner.
References: ISACA CISM Review Manual (Program management-risk response and operational controls); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 202
Which of the following is the BEST way to evaluate the effectiveness of physical and environmental security controls implemented for fire-related disasters?
A. Conduct evacuation exercises
B. Review the disaster recovery plan (DRP)
C. Conduct awareness sessions
D. Review emergency management team procedures
Answer: (SHOW ANSWER)
Evacuation drills provide real-time validation of physical security measures, staff preparedness, and response time during fire-related scenarios. They test both people and systems.
"Simulated exercises are the most effective method to evaluate real-world preparedness and the adequacy of response procedures."
- CISM Review Manual 15th Edition, Chapter 3: Security Controls Testing* Paper reviews and awareness are useful, but only exercises reveal actual gaps in preparedness.

NEW QUESTION: 203
The PRIMARY advantage of single sign-on (SSO) is that it will:
A. increase efficiency of access management
B. increase the security of related applications.
C. strengthen user passwords.
D. support multiple authentication mechanisms.
Answer: (SHOW ANSWER)
Single sign-on (SSO) is a technology that allows users to access multiple applications or services with one set of credentials, such as a username and password. The primary advantage of SSO is that it increases the efficiency of access management, as it reduces the need for users to remember and enter multiple passwords for different applications or services. SSO also simplifies the user experience, as they can log in once and access multiple resources without having to switch between different windows or tabs. SSO can also improve the security of related applications, as it reduces the risk of password compromise or phishing attacks.
However, SSO does not strengthen user passwords or support multiple authentication mechanisms by itself. It is a complementary technology that enhances the security and convenience of access management. References = CISM Review Manual, 16th Edition, page 991
The primary advantage of single sign-on (SSO) is that it increases the efficiency of access management. With SSO, users only need to remember one set of credentials to access all of their applications, rather than having to remember multiple usernames and passwords for each application. This simplifies the user experience and helps to reduce the amount of time spent

managing access to multiple applications. Additionally, SSO can also increase the security of related applications, as users are not sharing the same credentials across multiple applications, and it can also support multiple authentication mechanisms, such as biometric authentication.

NEW QUESTION: 204
Which of the following would be MOST helpful when creating information security policies?
A. The information security framework
B. Business impact analysis (BIA)
C. Information security metrics
D. Risk assessment results
Answer: (SHOW ANSWER)
The information security framework is a set of principles, standards, guidelines, and best practices that define the scope, objectives, and requirements for information security in an organization. The information security framework is most helpful when creating information security policies because it provides a consistent and coherent approach to managing information security risks, aligning with business goals and strategy, and complying with relevant laws and regulations. The information security framework also helps to establish the roles, responsibilities, and accountability of all stakeholders involved in information security governance, management, and operations.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Information Security Framework2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1

NEW QUESTION: 205
Which of the following is the BEST course of action when using a web application that has known vulnerabilities?
A. Monitor application level logs.
B. Install anti-spyware software.
C. Deploy host-based intrusion detection.
D. Deploy an application firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?
A. The application does not use a secure communications protocol
B. The application is configured with restrictive access controls
C. The business process has only one level of error checking
D. Server-based malware protection is not enforced

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 207

Which of the following BEST supports the adoption of effective information security practices throughout an organization?

A. Business continuity measures

B. A security-aware culture

C. The latest security technologies

D. Information security metrics

Answer: (SHOW ANSWER)

The correct answer is B because a security-aware culture encourages employees, managers, and stakeholders to consistently apply secure behaviors in daily operations. Effective security practices are adopted throughout an organization when people understand their responsibilities, recognize threats, and view security as part of business operations. Business continuity measures are important for resilience, but they do not broadly drive day-to-day adoption of security practices. The latest security technologies may improve technical protection, but technology alone cannot ensure people follow secure processes. Information security metrics help monitor and report performance, but they do not by themselves create behavioral adoption. CISM emphasizes that information security governance depends on culture, leadership, communication, awareness, and accountability. A security-aware culture supports compliance with policies, timely reporting of incidents, protection of information assets, and consistent risk-based decision-making. Therefore, among the available choices, a security-aware culture best supports effective organization-wide adoption of information security practices.

Reference: CISM Information Security Governance; security culture, awareness, communication, and organizational adoption principles.

NEW QUESTION: 208
When evaluating vendors for sensitive data processing, which of the following should be the FIRST step to ensure the correct level of information security is provided?
A. Include information security clauses in the vendor contract.
B. Review third-party reports of potential vendors.
C. Develop metrics for vendor performance.
D. Include information security criteria as part of vendor selection.
Answer: (SHOW ANSWER)
The first step is to include information security criteria as part of vendor selection (D). CISM third-party risk management guidance stresses that security requirements must be defined before contracting or performance measurement. Contracts (A), reports (B), and metrics (C) are ineffective if the vendor was not selected based on the organization's security needs. Embedding security criteria early ensures only vendors capable of meeting required controls, compliance, and risk thresholds are considered.
References: ISACA CISM Review Manual (Governance-third-party risk management); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 209
An organization is experiencing a sharp increase in incidents related to phishing messages. The root cause is an outdated email filtering system that is no longer supported by the vendor. Which of the following should be the information security manager's FIRST course of action?
A. Reinforce security awareness practices for end users.
B. Temporarily outsource the email system to a cloud provider.
C. Develop a business case to replace the system.
D. Monitor outgoing traffic on the firewall.
Answer: (SHOW ANSWER)
Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics." Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's

primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages." Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

NEW QUESTION: 210

When taking a risk-based approach to vulnerability management, which of the following is MOST important to consider when prioritizing a vulnerability?

Freecram.net

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: 211
Which of the following should be done FIRST to ensure information security is integrated into system development projects?
A. Define security requirements
B. Assign resources based on the business impact
C. Review the security policy
D. Embed a security representative in each project team
Answer: (SHOW ANSWER)
The correct answer is A because security must be defined as a requirement early in system development projects. Security requirements translate business, regulatory, privacy, risk, and control expectations into specific project deliverables. When requirements are defined early, security can be built into architecture, design, development, testing, and deployment. If requirements are not defined at the beginning, security may be added later as a costly or incomplete afterthought. Assigning resources based on business impact is useful, but resource

planning should follow a clear understanding of the required security outcomes. Reviewing the security policy may provide guidance, but it does not by itself integrate security into the project. Embedding a security representative can support integration, but the representative still needs defined requirements to guide the project team. CISM program management emphasizes integrating information security into life cycle processes and business initiatives as early as possible. Therefore, defining security requirements is the first and most important step to ensure security is built into system development projects.
Reference: CISM Information Security Program Development and Management; SDLC security, security requirements, project integration, and secure development principles.

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

NEW QUESTION: 212
Senior management is concerned about data exposure through the use of public AI services. Which of the following is the information security manager's BEST course of action?
A. Perform a business impact analysis (BIA) of public AI.
B. Disable access to public AI from company devices.
C. Train all employees on the appropriate use of public AI services and confidential data.
D. Perform a risk assessment of public AI with appropriate recommendations for senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Which of the following BEST minimizes information security risk in deploying applications to the production environment?
A. Integrating security controls in each phase of the life cycle
B. Conducting penetration testing post implementation
C. Having a well-defined change process
D. Verifying security during the testing process
Answer: (SHOW ANSWER)
= Integrating security controls in each phase of the life cycle is the best way to minimize information security risk in deploying applications to the production environment. This ensures that security requirements are defined, designed, implemented, tested, and maintained throughout the development process. Conducting penetration testing post implementation, having

a well-defined change process, and verifying security during the testing process are all important activities, but they are not sufficient to address all the potential risks that may arise during the application life cycle. Penetration testing may reveal some vulnerabilities, but it cannot guarantee that all of them are identified and fixed. A change process may help to control and document the modifications made to the application, but it does not ensure that the changes are secure and do not introduce new risks. Verifying security during the testing process may help to validate the functionality and performance of the security controls, but it does not ensure that the security requirements are complete and consistent with the business objectives and the risk appetite of the organization. References = CISM Review Manual, 16th Edition, page 1121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462

NEW QUESTION: 214
Which of the following is MOST important for a healthcare organization to address during the requirements gathering phase of AI development?
A. Algorithm selection challenges
B. Data privacy concerns
C. Inadequate computational resources
D. Data labeling inefficiencies
Answer: (SHOW ANSWER)
The most important consideration during the requirements gathering phase of AI development in a healthcare organization is data privacy concerns (B). From a CISM governance and risk management perspective, healthcare organizations handle highly sensitive personal and regulated data, such as protected health information (PHI), which is subject to strict privacy, confidentiality, and regulatory requirements. During requirements gathering, it is critical to ensure that legal, regulatory, and ethical obligations related to data use, retention, consent, access controls, and cross-border processing are fully understood and incorporated into system requirements.
Algorithm selection (A), computational resources (C), and data labeling efficiencies (D) are important technical and operational considerations, but they are secondary and should be addressed only after privacy requirements are clearly defined. CISM emphasizes that security and privacy must be built in by design, not retrofitted later in development. Failure to address privacy requirements early can result in regulatory noncompliance, reputational damage, and unacceptable risk exposure.
In healthcare, governance-driven requirements-especially privacy, data minimization, and lawful processing-must guide AI system design to ensure alignment with organizational risk appetite and compliance obligations.
References:
ISACA CISM Review Manual, Information Security Governance - privacy, regulatory compliance, and emerging technology risk ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 215
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: 216
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: (SHOW ANSWER)
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: 217
When developing a business case to justify an information security investment, which of the following would BEST enable an informed decision by senior management?
A. The information security strategy
B. Losses due to security incidents

C. The results of a risk assessment
D. Security investment trends in the industry
Answer: (SHOW ANSWER)
The results of a risk assessment would best enable an informed decision by senior management when developing a business case to justify an information security investment. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the organization's assets and processes, as well as the potential impact and likelihood of occurrence. A risk assessment will also provide a basis for selecting and evaluating the effectiveness of controls to mitigate the risks. According to CISA, developing a business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment1. The information security strategy, losses due to security incidents, and security investment trends in the industry are possible inputs or outputs of a risk assessment, but they are not sufficient to enable an informed decision by senior management. References: 1: The Business Case for Security - CISA 2: The Business Case for Security | CISA 3: #HowTo: Build a Business Case for Cybersecurity Investment 4: Making the Business Case for Information Security

NEW QUESTION: 218
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: 219
When drafting the corporate privacy statement for a public website, which of the following MUST be included?

A. Limited liability clause
B. Explanation of information usage
C. Information encryption requirements
D. Access control requirements
Answer: (SHOW ANSWER)
A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

NEW QUESTION: 220
An information security manager has recently been notified of potential security risks associated with a third- party service provider. What should be done NEXT to address this concern?
Freecram.net
A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.
D. Determine compensating controls.
Answer: (SHOW ANSWER)
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third- party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION: 221
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: (SHOW ANSWER)
= 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: 222
Which of the following is a prerequisite for formulating a business continuity plan (BCP)?
A. Recovery time objectives (RTOs) for the business processes
B. Process maps for production applications
C. System recovery procedures for alternate-site processing
D. Comprehensive property inventory
Answer: (SHOW ANSWER)
Recovery time objectives (RTOs) (A) are a prerequisite for developing a BCP because they define how quickly critical business processes must be restored. CISM clearly identifies the business impact analysis (BIA) and its outputs-such as RTOs-as foundational inputs to continuity planning. Recovery procedures (C) and process maps (B) are developed after recovery requirements are known. Property inventories (D) support asset management but are not central to BCP formulation.
References: ISACA CISM Review Manual (Program management-BCP and BIA); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 223
Which of the following roles is accountable for the protection of data?
A. CISO
B. Data custodian
C. Data owner
D. Data administrator
Answer: C (LEAVE A REPLY)
Under CISM governance principles, the data owner is accountable for the protection of data. Accountability includes decisions regarding data classification, access authorization, acceptable use, retention, and risk acceptance. While the CISO (A) provides oversight and guidance, they are not accountable for individual data assets. Data custodians (B) and administrators (D) are

responsible for implementing and operating controls but do not own the business risk associated with the data. CISM clearly distinguishes accountability (business) from responsibility (operational/technical). Assigning accountability to the data owner ensures that protection requirements align with business value, regulatory obligations, and risk appetite.
References: ISACA CISM Review Manual (Governance-roles and responsibilities, information asset ownership); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 224
Network sniffing is difficult to detect because it can be performed:
A. Passively.
B. Continuously.
C. Actively.
D. Remotely.
Answer: (SHOW ANSWER)
Network sniffing is difficult to detect primarily because it can be performed passively. In CISM terms, a passive attack is one in which the attacker monitors or intercepts data without altering system resources or network traffic patterns. Because passive sniffing does not generate abnormal traffic, modify packets, or interact directly with target systems, it often leaves no observable indicators that traditional security monitoring tools can easily detect.
CISM distinguishes between passive and active attacks, emphasizing that passive techniques such as packet sniffing, eavesdropping, and traffic analysis are inherently harder to identify than active attacks, which disrupt operations or modify data. Continuous operation (B) does not explain detectability, active sniffing (C) would generate detectable anomalies, and remote execution (D) does not inherently make detection more difficult.
From an incident management and detection perspective, this highlights the importance of preventive controls, such as encryption, secure network design, and segmentation, rather than relying solely on detection mechanisms. Because passive sniffing exploits visibility rather than system weakness, prevention is the primary risk mitigation strategy.
References:
ISACA CISM Review Manual, Information Security Incident Management - attack types and detection challenges ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 225
Which of the following is MOST important to the ongoing success of an information security program?
A. Executive sponsorship
B. Skilled personnel
C. Process automation
D. Regular awareness training
Answer: (SHOW ANSWER)

Executive sponsorship (A) is the most critical factor for the long-term success of an information security program. CISM emphasizes that leadership support enables funding, enforcement, cross-functional cooperation, and cultural adoption. Skilled staff (B), automation (C), and training (D) are important but depend on sustained executive backing to remain effective. Without sponsorship, security initiatives often lack authority and momentum.
References: ISACA CISM Review Manual (Governance-leadership and sponsorship); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 226
The PRIMARY purpose for deploying information security metrics is to:
A. compare program effectiveness to benchmarks.
B. ensure that technical operations meet specifications.
C. support ongoing security budget requirements.
D. provide information needed to make decisions.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 227
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: (SHOW ANSWER)
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: 228
Which of the following BEST enables the design of an effective incident escalation process?
A. Enforceable control baselines
B. Controls designed for defense in depth
C. A well-defined organizational hierarchy
D. A comprehensive risk register
Answer: (SHOW ANSWER)
A well-defined organizational hierarchy best enables the design of an effective incident escalation process.
Incident escalation requires clarity about authority, reporting paths, decision-making responsibility, and communication channels. CISM incident management emphasizes that response processes must define roles, responsibilities, thresholds, and escalation procedures before incidents occur. Without a clear organizational hierarchy, incidents may be delayed, misrouted, or escalated to personnel without appropriate authority.
Enforceable control baselines and defense-in-depth controls are important for prevention and security consistency, but they do not define escalation paths. A comprehensive risk register supports risk management but does not by itself establish who must be notified or who can make response decisions during an incident.
Escalation must align with the organization's management structure so that operational, legal, communications, and executive decisions can be made quickly. Therefore, a well-defined organizational hierarchy is the strongest foundation for an effective escalation process.
References:
ISACA CISM Review Manual , Information Security Incident Management - escalation, roles, and responsibilities ISACA CISM Exam Content Outline , Domain 4: Information Security Incident Management

NEW QUESTION: 229
The PRIMARY purpose of conducting a business impact analysis (BIA) is to determine the:
A. scope of the incident response plan.
B. scope of the business continuity program.
C. resources needed for business recovery.
D. recovery time objective (RTO).
Answer: (SHOW ANSWER)

NEW QUESTION: 230
When investigating an information security incident, details of the incident should be shared:
A. widely to demonstrate positive intent.
B. only with management.
C. only as needed,

D. only with internal audit.

Answer: (SHOW ANSWER)

When investigating an information security incident, details of the incident should be shared only as needed, according to the principle of least privilege and the need-to-know basis. This means that only the authorized and relevant parties who have a legitimate purpose and role in the incident response process should have access to the incident information, and only to the extent that is necessary for them to perform their duties.

Sharing incident details only as needed helps to protect the confidentiality, integrity, and availability of the incident information, as well as the privacy and reputation of the affected individuals and the organization.

Sharing incident details only as needed also helps to prevent unauthorized disclosure, modification, deletion, or misuse of the incident information, which could compromise the investigation, evidence, remediation, or legal actions.

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

10th Edition, Question 49, page 462.

NEW QUESTION: 231

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager?

A. Managing the impact

B. Identifying unacceptable risk levels

C. Assessing vulnerabilities

D. Evaluating potential threats

Answer: (SHOW ANSWER)

When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. References:

https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/

https://www.osha.gov/safety-management/hazard-prevention

https://www.cdc.gov/niosh/topics/hierarchy/default.html

NEW QUESTION: 232

Which of the following BEST determines the allocation of resources during a security incident response?

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

NEW QUESTION: 233
Which of the following is MOST helpful for determining which information security policies should be implemented by an organization?
A. Risk assessment
B. Business impact analysis (BIA)
C. Vulnerability assessment
D. Industry best practices
Answer: (SHOW ANSWER)
Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes1. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance2.
Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.
A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses3. A risk assessment helps to determine the following aspects of information security policies:
The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.

The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses.
The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.
The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.
The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations:
A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.
A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls.
Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.
References = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page
30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

NEW QUESTION: 234
An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?
A. Identification of risk

B. Analysis of control gaps
C. Design of key risk indicators (KRIs)
D. Selection of risk treatment options
Answer: (SHOW ANSWER)
= Identification of risk is the first and most important step in the IT risk management process, especially when the organization is undergoing a digital transformation that introduces new technologies, processes, and business models. Identification of risk involves determining the sources, causes, and potential consequences of IT-related risks that may affect the organization's objectives, assets, and stakeholders. Identification of risk also helps to establish the risk context, scope, and criteria for the subsequent risk analysis, evaluation, and treatment. Without identifying the risks, the information security manager cannot effectively assess the risk exposure, prioritize the risks, implement appropriate controls, monitor the risk performance, or communicate the risk information to the relevant parties.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, page 841; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
34, page 352.

NEW QUESTION: 235
An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?
A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.
Answer: C (LEAVE A REPLY)
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION: 236

Which of the following MOST directly influences the efficiency of incident response immediately after an incident has been detected?

A. Incident containment and mitigation

B. Root cause analysis

C. Incident categorization

D. Lessons learned

Answer: (SHOW ANSWER)

The correct answer is C because incident categorization directly influences how efficiently the organization responds immediately after detection. Categorization helps determine the type of incident, severity, priority, required resources, escalation path, communication requirements, and expected response procedure. Without quick and accurate categorization, responders may waste time deciding who should act, how urgent the situation is, and what containment actions are appropriate. Containment and mitigation are critical response activities, but they depend on proper categorization and prioritization. Root cause analysis is normally performed later to determine why the incident occurred and how to prevent recurrence. Lessons learned are also post-incident activities used to improve future response. CISM incident management emphasizes that detected incidents should be analyzed, classified, prioritized, and escalated based on impact and urgency. This allows the organization to apply the right response playbook quickly and use resources effectively. Therefore, incident categorization most directly improves response efficiency immediately after detection.

Reference: CISM Information Security Incident Management; incident categorization, classification, prioritization, escalation, and response efficiency principles.

NEW QUESTION: 237

An organization recently identified a significant risk related to data exfiltration, and the information security manager is asked to quickly address this issue. The security team suggests a number of different security controls. Which of the following is the BEST approach for selecting controls to manage the risk?

A. Implement controls recommended by an industry-recognized security framework.

B. Assess the effectiveness of each control in reducing residual risk.

C. Prioritize the controls based on ease of implementation and resource availability.

D. Choose the most economical controls for risk mitigation based on a cost-benefit analysis.

Answer: (SHOW ANSWER)

The best approach for selecting security controls is to assess the effectiveness of each control in reducing residual risk (B). CISM emphasizes that control selection must be risk-based and outcome-focused, with the primary objective of reducing risk to within the organization's defined risk appetite. When multiple controls are available, the information security manager should evaluate how well each option mitigates the identified risk-specifically data exfiltration-and determine the resulting residual risk after implementation.

Implementing controls solely because they are recommended by a framework (A) may not adequately address the organization's specific threat scenario or business context. Prioritizing

controls based on ease of implementation or available resources (C) shifts focus away from risk reduction and may result in insufficient protection. Cost-benefit analysis (D) is an important supporting activity, but in CISM it is secondary to understanding risk reduction effectiveness. CISM guidance consistently states that security controls should be selected based on their ability to reduce risk exposure in a measurable and meaningful way, ensuring alignment with business objectives, risk tolerance, and governance expectations.
References:
ISACA CISM Review Manual, Information Risk Management - risk treatment and control selection
ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

NEW QUESTION: 238
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: 239
Which of the following is the GREATEST concern with implementing all controls recommended by a security framework?
A. Increased time for implementation
B. Lack of approval from senior management
C. Negative return on investment
D. Increased risk levels
Answer: C (LEAVE A REPLY)
The correct answer is C because implementing every control recommended by a security framework without considering business risk, cost, value, and applicability may lead to excessive spending and negative return on investment. Security frameworks provide useful guidance, but they are not intended to be applied blindly.
Controls should be selected based on the organization's risk profile, regulatory requirements, business objectives, risk appetite, and cost-benefit considerations. Increased implementation time is possible, but it is not the greatest concern if controls are justified by risk. Lack of senior management approval is a governance issue, but the deeper concern is that unnecessary controls may consume resources without reducing meaningful risk. Increased risk levels are unlikely to result directly from implementing more controls, although poorly implemented controls can create operational issues. In CISM, information security programs should deliver value by managing risk cost-effectively. Implementing all framework controls may waste resources and reduce program efficiency. Therefore, negative return on investment is the greatest concern.
Reference: CISM Information Security Program Development and Management; control selection, cost- benefit analysis, security frameworks, and value delivery principles.

NEW QUESTION: 240
Which of the following is the GREATEST threat posed by quantum computing technology for information security?
Freecram.net
A. Quantum computers can break several current encryption schemes protecting the confidentiality of data
B. Quantum computers can allow for secure communication that benefits only the few who can afford it
C. Quantum computers can compromise availability through extremely rapid processing of large data sets
D. Quantum computers can simulate complex physical systems beyond traditional computing capabilities
Answer: (SHOW ANSWER)
The greatest threat posed by quantum computing is its potential to break widely used cryptographic algorithms (A), particularly public-key encryption schemes that rely on

mathematical problems vulnerable to quantum algorithms. This directly threatens data confidentiality and long-term data protection. The other options describe secondary or non-security impacts. CISM recognizes cryptographic resilience as a core component of risk management and emphasizes the need for organizations to monitor emerging technologies that could invalidate existing controls. Quantum computing's impact on encryption represents a systemic risk to trust, privacy, and secure communications.
References: ISACA CISM Review Manual (Risk management-emerging technologies and cryptographic risk); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 241
An international organization with remote branches is implementing a corporate security policy for managing personally identifiable information (PII). Which of the following should be the information security manager's MAIN concern?
A. Local regulations
B. Data backup strategy
C. Consistency in awareness programs
D. Organizational reporting structure
Answer: (SHOW ANSWER)
Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

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

NEW QUESTION: 242
Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.
Answer: (SHOW ANSWER)
= Residual risk is the risk that remains after applying security controls. It reflects the actual exposure of the organization to noncompliance issues. Therefore, basing mandatory review and exception approvals on residual risk is the best approach for governing noncompliance with security requirements. It ensures that the organization is aware of the potential impact and likelihood of noncompliance and can make informed decisions about accepting, mitigating, or transferring the risk. References = CISM Review Manual 15th Edition, page 78.

NEW QUESTION: 243
What is the role of the information security manager in finalizing contract negotiations with service providers?
A. To perform a risk analysis on the outsourcing process
B. To obtain a security standard certification from the provider
C. To update security standards for the outsourced process
D. To ensure that clauses for periodic audits are included
Answer: (SHOW ANSWER)
The role of the information security manager in finalizing contract negotiations with service providers is to ensure that the outsourcing process is aligned with the organization's information security policies, standards, and objectives. One of the key aspects of this process is to perform a risk analysis on the outsourcing process, which involves identifying, assessing, and mitigating the potential threats and vulnerabilities that may arise from outsourcing activities. A risk analysis can help the information security manager to determine the appropriate level of security controls and requirements for the outsourced process, as well as to monitor and evaluate its performance and compliance. A risk analysis can also help to avoid or minimize legal, financial, reputational, or operational risks associated with outsourcing1. References = CISM Review Manual (Digital Version), Chapter 6: Information Security Program Management CISM Review Manual (Print Version), Chapter 6: Information Security Program Management

NEW QUESTION: 244
Which of the following is the PRIMARY objective of testing security controls within a critical infrastructure?
A. Identifying and addressing security team performance issues
B. Reducing the number of control assessments to optimize resources
C. Decreasing the percentage of security deployments that cause failures in production
D. Ensuring the continued resilience and security of IT services
Answer: (SHOW ANSWER)

NEW QUESTION: 245
Which of the following is the MOST critical factor for information security program success?
A. comprehensive risk assessment program for information security
B. The information security manager's knowledge of the business
C. Security staff with appropriate training and adequate resources
D. Ongoing audits and addressing open items
Answer: (SHOW ANSWER)
The explanation given in the manual is:
The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.
An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

NEW QUESTION: 246
Which of the following is the MOST effective control to prevent proliferation of shadow IT?
A. Install a solution to detect unlicensed software.
B. Conduct software audits.
C. Implement a software allow list.
D. Conduct periodic vulnerability scanning.
Answer: (SHOW ANSWER)
The most effective control to prevent the proliferation of shadow IT is implementing a software allow list.
From a CISM governance perspective, shadow IT represents the use of unauthorized applications and technologies outside established governance and approval processes, which increases risk exposure and undermines control effectiveness. CISM emphasizes that preventive controls are superior to detective controls when the objective is to stop undesirable behavior before it occurs.
A software allow list enforces policy by ensuring that only approved and authorized applications can be installed or executed, directly preventing users from introducing unapproved tools. In contrast, detecting unlicensed software (A) and conducting software audits (B) are detective controls that identify shadow IT only after it has already been deployed. Periodic vulnerability scanning (D) focuses on identifying technical weaknesses, not unauthorized software usage, and therefore does not address the root cause of shadow IT.

CISM guidance stresses aligning technical controls with governance policies to ensure consistent enforcement and risk reduction. Allow listing operationalizes policy requirements and supports management's intent by embedding control directly into system operation.
References:
ISACA CISM Review Manual, Information Security Governance - policy enforcement and preventive controls ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 247
Which of the following is the MOST important consideration for an incident response team seeking to limit the impact of incidents?
A. Senior management's understanding of the risk appetite
B. Year-to-year analysis of incident response training completion
C. Understanding of the organization's operational requirements
D. Allocation of funding assigned to incident management functions
Answer: (SHOW ANSWER)
The correct answer is C because an incident response team can limit impact most effectively when it understands the organization's operational requirements, including critical systems, business priorities, dependencies, acceptable downtime, data sensitivity, and service restoration needs. Incident response decisions often require balancing containment with business continuity. For example, disconnecting a system may stop an attack but could also interrupt critical operations. Understanding operational requirements enables the team to choose response actions that reduce security impact while minimizing disruption to essential business activities.
Senior management's understanding of risk appetite is important for governance, but the response team needs practical operational knowledge during incidents. Training completion trends are useful for program monitoring, but they do not directly guide impact-limiting decisions during an event.
Funding supports capability, but it is not the most immediate consideration during response.
CISM incident management emphasizes business impact reduction, coordinated response, prioritization, and restoration of critical services. Therefore, understanding operational requirements is the most important consideration for limiting incident impact.
Reference: CISM Information Security Incident Management; incident response prioritization, business impact, operational requirements, and impact limitation principles.

NEW QUESTION: 248
Which of the following methods is the BEST way to demonstrate that an information security program provides appropriate coverage?
A. Security risk analysis
B. Gap assessment
C. Maturity assessment
D. Vulnerability scan report

Answer: (SHOW ANSWER)

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

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

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

Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1015.

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

NEW QUESTION: 249

It is MOST important that risk owners understand they are accountable for:

A. Overseeing and monitoring the effectiveness of controls associated with the risk

B. Collaborating with stakeholders to evaluate the effectiveness of controls associated with the risk

C. Reporting risk metrics and control compliance status to the information security manager

D. Escalating control deficiencies associated with the risk to the steering committee for decision making

Answer: (SHOW ANSWER)

NEW QUESTION: 250

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: 251
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: 252
Which of the following is the PRIMARY benefit of implementing an information security governance framework?
A. The framework defines managerial responsibilities for risk impacts to business goals.
B. The framework provides direction to meet business goals while balancing risks and controls.
C. The framework provides a roadmap to maximize revenue through the secure use of technology.
D. The framework is able to confirm the validity of business goals and strategies.
Answer: (SHOW ANSWER)
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: 253
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: (SHOW ANSWER)
= 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: 254
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: 255
Which of the following should an organization do FIRST upon learning that a subsidiary is located in a country where civil unrest has just begun?
A. Assess changes in the risk profile.
B. Conduct security awareness training.
C. Activate the disaster recovery plan (DRP).
D. Invoke the incident response plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 256
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: (SHOW ANSWER)
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

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

NEW QUESTION: 257
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders
Answer: (SHOW ANSWER)
= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them.
By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION: 258
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: (SHOW ANSWER)

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: 259
Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?
A. Demonstrating the program's value to the organization
B. Discussing governance programs found in similar organizations
C. Providing the results of external audits
D. Providing examples of information security incidents within the organization
Answer: (SHOW ANSWER)
The best way to obtain senior management support for an information security governance program is to demonstrate the program's value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. References:
* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process
* https://www.sans.org/white-papers/992/
* https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for-your- security-program.html

NEW QUESTION: 260
Which of the following metrics would provide an accurate measure of an information security program's performance?
Freecram.net

A. A collection of qualitative indicators that accurately measure security exceptions
B. A combination of qualitative and quantitative trends that enable decision making
C. A collection of quantitative indicators that are compared against industry benchmarks
D. A single numeric score derived from various measures assigned to the security program
Answer: (SHOW ANSWER)

NEW QUESTION: 261
Which type of control is an incident response team?
A. Corrective
B. Directive
C. Detective
D. Preventive
Answer: (SHOW ANSWER)

NEW QUESTION: 262
In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:
A. evaluate results of the most recent incident response test.
B. review the number of reported security incidents.
C. ensure established security metrics are reported.
D. assess progress of risk mitigation efforts.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, an organization's security posture is the overall condition of its information security, which is determined by the effectiveness of its security program and the alignment of its security objectives with its business goals. To understand the security posture, the senior leadership needs to have a holistic view of the security risks and the actions taken to address them. Therefore, assessing the progress of risk mitigation efforts is the most important activity for the senior leadership, as it provides them with the information on how well the security program is performing and whether it is meeting the expected outcomes. Evaluating the results of the most recent incident response test, reviewing the number of reported security incidents, and ensuring established security metrics are reported are all useful activities for the senior leadership, but they are not sufficient to understand the security posture. They only provide partial or isolated information on the security performance, which may not reflect the overall security condition or the alignment with the business objectives. References = CISM Review Manual, 16th Edition, Chapter 1, Information Security Governance, pages 28-29.

NEW QUESTION: 263
The fundamental purpose of establishing security metrics is to:
A. increase return on investment (ROI)
B. provide feedback on control effectiveness
C. adopt security best practices

D. establish security benchmarks

Answer: (SHOW ANSWER)

The fundamental purpose of establishing security metrics is to provide feedback on the effectiveness of the information security controls and processes. Security metrics are quantitative or qualitative measures that indicate how well the organization is achieving its security objectives and goals. Security metrics can help the information security manager to monitor, evaluate, and improve the performance of the information security program, as well as to identify gaps, weaknesses, and areas for improvement. Security metrics can also help the organization to demonstrate compliance with internal and external standards, regulations, and best practices. Increasing return on investment (ROI), adopting security best practices, and establishing security benchmarks are possible outcomes or benefits of using security metrics, but they are not the fundamental purpose of establishing them. References = CISM Review Manual, 16th Edition, pages 46-471; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 642

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Security metrics are used to measure the effectiveness of controls and evaluate the overall security posture of an organization. This feedback provides an understanding of the progress made towards achieving security objectives and allows organizations to make necessary adjustments.

NEW QUESTION: 264

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

A. Communicating with the management team

B. Integrating staff with the IT department

C. Testing response scenarios

D. Reviewing the incident response plan annually

Answer: (SHOW ANSWER)

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

The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to

handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents.
However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions.
References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

NEW QUESTION: 265
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: (SHOW ANSWER)
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: 266
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: 267
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. Laws and regulations of the origin country may not be applicable.
B. Labeling of data may help to ensure data is assigned to the correct cloud type.
C. There may be liabilities and penalties in the event of a security breach.
D. Data may be stored in unknown locations and may not be easily retrievable.
Answer: (SHOW ANSWER)

NEW QUESTION: 268
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: (SHOW ANSWER)

NEW QUESTION: 269
Which of the following is the BEST reason for delaying the application of a critical security patch?
A. Conflicts with the software development life cycle
B. Lack of vulnerability management
C. Resource limitations
D. Technology interdependencies
Answer: (SHOW ANSWER)
The best reason for delaying a critical security patch is technology interdependencies . CISM recognizes that patching must be risk-based, but also controlled to avoid creating operational outages or failures in dependent systems. Critical patches should generally be applied promptly; however, if a patch may disrupt interconnected applications, infrastructure, or business-critical services, the organization may need to test, coordinate, and implement temporary compensating controls before deployment. Conflicts with the software development life cycle are not a strong reason to delay a critical security patch because emergency change processes should exist. Lack of vulnerability management is a program weakness, not a valid justification.
Resource limitations may explain a delay but do not represent a sound security rationale for accepting increased exposure. Technology interdependencies can create unacceptable availability or integrity impacts if not managed carefully. Therefore, delaying the patch may be justified only to ensure safe implementation while managing the interim risk through approved risk treatment and compensating controls.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - patch management, change control, and compensating controls ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 270
Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?
Freecram.net
A. Increase the frequency of system backups.
B. Review the mitigating security controls.
C. Notify staff members of the threat.
D. Assess the risk to the organization.

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

NEW QUESTION: 271
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 ensure system audit trails are not bypassed
B. To prevent unauthorized user access
C. To ensure separation of duties is maintained
D. To prevent accountability issues
Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 272
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: (SHOW ANSWER)
Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.
Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.
However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. References = CISM Review Manual,
16th Edition, Chapter 5, Section 5.4.1.2

NEW QUESTION: 273
Which of the following has the GREATEST influence on the successful integration of information security within the business?
A. Organizational structure and culture
B. Risk tolerance and organizational objectives
C. The desired state of the organization
D. Information security personnel
Answer: (SHOW ANSWER)
The factor that has the greatest influence on the successful integration of information security within the business is organizational structure and culture because they determine how information security is organized, governed, and supported within the organization, and how information security roles and responsibilities are defined, assigned, and communicated across different levels and functions. Risk tolerance and organizational objectives are not very influential because they do not affect how information security is integrated within the business, but rather what information security aims to achieve or protect. The desired state of the organization is not very influential because it does not affect how information security is integrated within the business, but rather what the organization aspires to be or do. Information security personnel are

not very influential because they do not affect how information security is integrated within the business, but rather who performs information security tasks or activities. References:
https://www.isaca.org/resources/isaca-journal/issues/2016
/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal
/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

NEW QUESTION: 274
Before approving the implementation of a new security solution, senior management requires a business case.
Which of the following would BEST support the justification for investment?
A. The solution contributes to business strategy.
B. The solution improves business risk tolerance levels.
C. The solution improves business resiliency.
D. The solution reduces the cost of noncompliance with regulations.
Answer: (SHOW ANSWER)
The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 275
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: (SHOW ANSWER)
= 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: 276

Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?

A. Perform a risk assessment.

B. Reduce security hardening settings.

C. Inform business management of the risk.

D. Document a security exception.

Answer: (SHOW ANSWER)

Security hardening is the process of applying security configuration settings to systems and software to reduce their attack surface and improve their resistance to threats1. Security hardening settings are based on industry standards and best practices, such as the CIS Benchmarks2, which provide recommended security configurations for various software applications, operating systems, and network devices. However, security hardening settings may not always be compatible with the business requirements and objectives of an organization, and may negatively impact the functionality, performance, or usability of the systems and software3. Therefore, before applying any security hardening settings, an information security manager should perform a risk assessment to evaluate the potential benefits and drawbacks of the settings, and to identify and prioritize the risks associated with them. A risk assessment is a

systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses.
A risk assessment helps the information security manager to balance the security and business needs of the organization, and to communicate the risk level and impact to the relevant stakeholders. A risk assessment should be performed first, before taking any other actions, such as reducing security hardening settings, informing business management of the risk, or documenting a security exception, because it provides the necessary information and justification for making informed and rational decisions. References = 1: Basics of the CIS Hardening Guidelines | RSI Security 2: CIS Baseline Hardening and Security Configuration Guide | CalCom 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 145 : CISM Review Manual 15th Edition, page 146 : CISM Review Manual 15th Edition, page 147

NEW QUESTION: 277
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: (SHOW ANSWER)
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: 278
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: (SHOW ANSWER)
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: 279
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 objectives
B. Information security threat profile
C. Information security policy
D. Information security strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 280
The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:
Freecram.net
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: 281
What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?
A. Developing a dashboard for communicating the metrics

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

NEW QUESTION: 282
An organization requires that business-critical applications be recovered within 30 minutes in the event of a disaster. Which of the following metrics should be defined in the business continuity plan (BCP) to manage this requirement?
A. Recovery time objective (RTO)
B. Recovery point objective (RPO)
C. Maximum tolerable downtime (MTD)
D. Service level agreement (SLA)
Answer: (SHOW ANSWER)
The Recovery Time Objective (RTO) specifies the maximum acceptable downtime before operations must resume. A 30-minute requirement directly defines the RTO for those systems.
"RTO defines the duration within which systems must be restored following an outage to prevent unacceptable business impact."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity Planning, Section: Continuity Metrics*

NEW QUESTION: 283
A business impact analysis (BIA) BEST enables an organization to establish:
A. total cost of ownership (TCO).
B. annualized loss expectancy (ALE).
C. recovery methods.
D. restoration priorities.
Answer: (SHOW ANSWER)

NEW QUESTION: 284

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

A. Define policies and standards for data processing.

B. Implement applicable privacy principles

C. Assess local or regional regulations

D. Research cyber insurance policies

Answer: (SHOW ANSWER)

Before transferring personal data across borders, an organization should first assess the local or regional regulations that apply to the data protection and privacy of the data subjects. This will help the organization to identify the legal requirements and risks involved in the data transfer, and to choose the appropriate tools and safeguards to ensure compliance and protection. For example, the organization may need to obtain consent from the data subjects, use adequacy decisions, standard contractual clauses, or other mechanisms to ensure an adequate level of protection in the third country, or rely on specific derogations for certain situations. The other options are not the first steps to take, although they may be relevant at later stages of the data transfer process. References = Guide to the cross-border transfer of personal data in the GDPR New guidance issued by the EDPB on international transfers of personal data Requirements for transferring personal information across borders

NEW QUESTION: 285

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: 286
Which of the following processes BEST supports the evaluation of incident response effectiveness?
A. Root cause analysis
B. Post-incident review
C. Chain of custody
D. Incident logging
Answer: (SHOW ANSWER)
A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement1. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity2.
A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders3.
A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.
The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization

ensure that the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the effectiveness of the response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation. However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices. References = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: Post-Incident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

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

NEW QUESTION: 287
Which of the following is the PRIMARY preventive method to mitigate risks associated with privileged accounts?
A. Frequently monitor activities on privileged accounts.
B. Perform periodic certification of access to privileged accounts.
C. Provide privileged account access only to users who need it.
D. Eliminate privileged accounts.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 288
Behavioral analytics tools are used PRIMARILY to manage risks within an organization by:
A. Preventing the exfiltration of sensitive data
B. Analyzing communications from external users for malware
C. Establishing security baselines on endpoints
D. Detecting anomalous user activities
Answer: (SHOW ANSWER)

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

NEW QUESTION: 289
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: 290

Which of the following should occur FIRST in the process of managing security risk associated with the transfer of data from unsupported legacy systems to supported systems?

Freecram.net

A. Perform security testing on legacy systems

B. Identify all information assets in the legacy environment

C. Assign owners to be responsible for the transfer of each asset

D. Conduct a business impact analysis (BIA)

Answer: (SHOW ANSWER)

The first step should be to identify all information assets in the legacy environment . Managing security risk during data transfer requires understanding what data and information assets exist before evaluating impact, assigning ownership, testing, or selecting controls. CISM risk management emphasizes that asset identification is foundational because organizations cannot protect, classify, transfer, or assign accountability for assets they do not know exist. A business impact analysis may help prioritize critical processes and recovery requirements, but it does not replace the need to identify the data assets being transferred. Security testing of legacy systems may be useful later, especially if the systems remain operational during migration, but it is not the first step. Assigning owners is necessary, but ownership can only be accurately assigned after assets are identified. Unsupported legacy systems often contain undocumented data, obsolete interfaces, and unknown dependencies. Therefore, the first risk management activity must be creating an accurate inventory of information assets in the legacy environment.

References:

ISACA CISM Review Manual , Information Risk Management - asset identification, classification, and risk assessment ISACA CISM Exam Content Outline , Domain 1: Information Risk Management

NEW QUESTION: 291

Which of the following would BEST enable the help desk to recognize an information security incident?

A. Train the help desk to review the call logs.

B. Require the help desk to participate in post-incident reviews.

C. Provide the help desk with criteria for security incidents.

D. Include members of the help desk on the security incident response team.

Answer: (SHOW ANSWER)

Providing the help desk with clear criteria for what constitutes a security incident (C) is the most effective way to enable early recognition. In CISM incident management, frontline functions such as the help desk are critical for early detection and escalation, but only if they understand what events require security attention.

Reviewing call logs (A) or participating in post-incident reviews (B) improves awareness after the fact, not recognition in real time. Including help desk staff on the response team (D) is unnecessary and impractical for incident identification. Clearly defined criteria and escalation thresholds empower the help desk to act quickly and consistently.

References: ISACA CISM Review Manual (Incident management-incident identification and escalation); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 292
To improve the efficiency of the development of a new software application, security requirements should be defined:
A. based on code review.
B. based on available security assessment tools.
C. after functional requirements.
D. concurrently with other requirements.
Answer: (SHOW ANSWER)
Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the organization, not on code review, security assessment tools, or functional requirements. References = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

NEW QUESTION: 293
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: 294

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: 295
Results from which of the following would BEST provide an understanding of the effectiveness of an organization's information security program?
A. Security spot checks
B. Internal audits
C. Enterprise risk assessments
D. Control self-assessments (CSAs)
Answer: (SHOW ANSWER)
Control self-assessments (CSAs) (D) best provide an understanding of the effectiveness of an organization's information security program because they focus specifically on whether security controls are operating as intended on an ongoing basis. In CISM, program effectiveness is measured not only by design adequacy, but by consistent execution and performance of controls across the organization.
CSAs enable control owners and business stakeholders to evaluate control implementation, identify weaknesses, and report effectiveness in a structured and repeatable manner. This provides management with broad, timely, and actionable insight into how well the security program is functioning day to day. Internal audits (B) offer independent assurance but are typically periodic and retrospective. Enterprise risk assessments (C) focus on identifying and prioritizing risks, not on validating control performance. Security spot checks (A) are limited in scope and do not provide a comprehensive program view.

CISM emphasizes that effective security programs rely on continuous monitoring and self-assessment mechanisms to demonstrate control effectiveness, support improvement, and inform governance reporting.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - monitoring, measurement, and control effectiveness ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 296
Which of the following should be the PRIMARY outcome of an information security program?
A. Strategic alignment
B. Risk elimination
C. Cost reduction
D. Threat reduction
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, strategic alignment is the primary outcome of an information security program1. Strategic alignment means that the information security program supports and is tailored to the organization's objectives and business strategy1. It also means that the information security program is aligned with other assurance functions, such as physical, human resources, quality, and IT1.
The CISM Review Manual (Digital Version) also states that strategic alignment is essential for achieving a competitive advantage, enhancing customer trust, reducing legal and regulatory risks, and improving organizational performance1. Strategic alignment requires effective communication and collaboration among all stakeholders, including senior management, information owners, information security managers, information security steering committees, and external partners1.
The CISM Exam Content Outline also covers the topic of strategic alignment in Domain 3 - Information Security Program Development and Management (33% exam weight)2. The subtopics include:
3.2.1 Information Security Strategy
3.2.2 Information Security Governance
3.2.3 Information Security Risk Management
3.2.4 Information Security Compliance
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 297
Which of the following is MOST useful to an information security manager when reporting the performance of the information security program to senior management?
A. Number of policy exceptions
B. Number of incidents identified and remediated
C. System vulnerability scan results
D. Results of an independent security audit

Answer: (SHOW ANSWER)
The correct answer is D because an independent security audit provides objective assurance about the performance and effectiveness of the information security program. Senior management needs reliable, high- level information to evaluate whether the program is achieving its objectives, managing risk appropriately, and supporting business goals. An independent audit can assess governance, controls, compliance, risk management, operations, and program maturity from an unbiased perspective. The number of policy exceptions is useful as a metric, but it gives only a narrow view of compliance behavior. The number of incidents identified and remediated may show operational activity, but it does not fully measure program effectiveness. Vulnerability scan results are technical and limited to specific systems or environments; they do not provide an enterprise-level view of program performance. CISM governance emphasizes management reporting, independent assurance, accountability, and performance evaluation. Therefore, among the listed options, independent security audit results are the most useful for reporting overall program performance to senior management.
Reference: CISM Information Security Governance; program reporting, independent assurance, audit results, and senior management oversight principles.

NEW QUESTION: 298
Which of the following would BEST help to ensure appropriate security controls are built into software?
A. Integrating security throughout the development process
B. Performing security testing prior to deployment
C. Providing standards for implementation during development activities
D. Providing security training to the software development team
Answer: (SHOW ANSWER)
The best way to ensure appropriate security controls are built into software is to integrate security throughout the development process. This means that security should be considered from the initial stages of planning, design, coding, testing, deployment, and maintenance of the software. Integrating security throughout the development process helps to identify and mitigate security risks early, reduce the cost and complexity of fixing vulnerabilities later, improve the quality and reliability of the software, and enhance the trust and confidence of the users and customers. Integrating security throughout the development process also aligns with the best practices and standards of information security governance, such as the CISM framework123.
References =
CISM Review Manual 15th Edition, page 1631
CISM domain 3: Information security program development and management [2022 update]2
CISSP domain 8 overview: Software development security4

NEW QUESTION: 299
Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?

A. Enforce the local regulation.
B. Obtain legal guidance.
C. Enforce the organization's information security policy.
D. Obtain an independent assessment of the regulation.
Answer: (SHOW ANSWER)
The information security manager should first obtain legal guidance when there is a conflict between the organization's information security policy and a local regulation, because this will help to understand the implications and consequences of the conflict, and to identify the possible options and solutions for resolving it. The information security manager should also consult with the relevant stakeholders, such as senior management, business owners, and information owners, to determine the best course of action that aligns with the organization's objectives, risk appetite, and compliance obligations. Enforcing the local regulation or the organization's information security policy without legal guidance may expose the organization to legal liabilities, security risks, or operational disruptions. Obtaining an independent assessment of the regulation may be helpful, but it is not the first step to take.
References = CISM Review Manual, 16th Edition, page 691; A Guide to ISACA CISM Domains & Domain
1: Information Security Governance2

NEW QUESTION: 300
Which of the following is MOST likely to reduce the effectiveness of a SIEM system?
A. Complex user interface
B. Misconfiguration of alert thresholds
C. Weakly encrypted log files
D. Lack of multi-factor authentication (MFA) for system access
Answer: (SHOW ANSWER)
The effectiveness of a SIEM (Security Information and Event Management) system heavily relies on properly configured alert thresholds. Misconfiguration of alert thresholds can result in missed detection of significant incidents (false negatives) or an overwhelming number of false positives, making it difficult to identify real threats. According to the CISM Review Manual, 16th Edition, Domain 4: Information Security Incident Management, the configuration and tuning of monitoring tools like SIEMs are crucial for timely and accurate detection of incidents.
Reference:ISACA CISM Review Manual, 16th Edition, Page 304-305, "Security Event Management Tools and Techniques".

NEW QUESTION: 301
Which of the following processes should be done NEXT after completing a business impact analysis (BIA)?
A. Develop the requirements for the incident response plan
B. Develop a business continuity plan (BCP)
C. Evaluate the disaster recovery plan (DRP)

D. Identify resources for business recovery

Answer: (SHOW ANSWER)

After completing a business impact analysis, the next step is to identify resources for business recovery .

The BIA identifies critical business processes, recovery priorities, impacts over time, recovery time objectives, and recovery point objectives. Once these requirements are known, the organization must determine the resources needed to meet them, such as personnel, facilities, technology, data, applications, vendors, and alternate processing capabilities. Developing a business continuity plan occurs after recovery requirements and resources are understood. Evaluating the disaster recovery plan would generally occur after plans have been developed and tested. Developing requirements for the incident response plan is related to incident management, but it is not the next step after a BIA in continuity planning. CISM program management emphasizes that BIA outputs drive recovery strategy development, and resource identification is a necessary bridge between impact analysis and actionable continuity plans. Therefore, identifying resources for business recovery is the appropriate next activity after the BIA.

References:

ISACA CISM Review Manual , Information Security Program Development and Management - BIA outputs and continuity strategy development ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

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

NEW QUESTION: 302

Which of the following is a function of the information security steering committee?

A. Align the security framework with security standards.

B. Deliver external communication during incident response.

C. Monitor regulatory requirements.

D. Align security strategy with business objectives.

Answer: (SHOW ANSWER)

NEW QUESTION: 303

An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

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

NEW QUESTION: 304
Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?
A. Availability of resources
B. Root cause analysis results
C. Adverse effects on the business
D. Legal and regulatory requirements
Answer: C (LEAVE A REPLY)
The severity hierarchy for information security incident classification should be based on the potential or actual impact of the incident on the business objectives, operations, reputation, and stakeholders. The adverse effects on the business can be measured by criteria such as financial

loss, operational disruption, legal liability, regulatory compliance, customer satisfaction, and public confidence. The other options are not the primary basis for a severity hierarchy, although they may be considered as secondary factors or consequences of an incident

NEW QUESTION: 305
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: (SHOW ANSWER)

NEW QUESTION: 306
An organization is considering the feasibility of implementing a big data solution to analyze customer data. In order to support this initiative, the information security manager should FIRST:
A. inventory sensitive customer data to be processed by the solution.
B. determine information security resource and budget requirements.
C. assess potential information security risk to the organization.
D. develop information security requirements for the big data solution.
Answer: (SHOW ANSWER)
Assessing potential information security risk to the organization is the first step that the information security manager should take when considering the feasibility of implementing a big data solution to analyze customer data, as it helps to identify and evaluate the threats, vulnerabilities, and impacts that may arise from the collection, processing, storage, and sharing of large volumes and varieties of customer data. Assessing risk also helps to determine the risk appetite and tolerance of the organization, and to prioritize the risk treatment options and security controls that are needed to protect the customer data and the big data solution. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Big Data Security and Privacy Issues in Healthcare1, page 1, section 1. Introduction.

NEW QUESTION: 307
Which of the following BEST indicates the organizational benefit of an information security solution?
A. Cost savings the solution brings to the information security department
B. Reduced security training requirements
C. Alignment to security threats and risks
D. Costs and benefits of the solution calculated over time
Answer: (SHOW ANSWER)
The best option to indicate the organizational benefit of an information security solution is D. Costs and benefits of the solution calculated over time. This is because costs and benefits of the

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

NEW QUESTION: 308
Which of the following is the BEST way to monitor the effectiveness of security controls?
A. Benchmark security controls against similar organizations
B. Review application and system audit logs
C. Establish and report security metrics
D. Conduct regular threat assessments
Answer: (SHOW ANSWER)
The correct answer is C because security metrics provide measurable evidence of whether controls are operating effectively and achieving intended outcomes. Establishing and reporting metrics allows the information security manager to monitor trends, identify control weaknesses, support management decisions, and demonstrate program performance. Benchmarking can provide useful external comparison, but it does not directly measure the organization's own control effectiveness. Reviewing audit logs is valuable for specific detective controls, but it is too narrow to monitor the overall effectiveness of security controls. Threat assessments help identify changing threat conditions, but they do not directly show whether controls are performing as intended. CISM emphasizes performance measurement, monitoring, and reporting as essential components of managing an information security program. Metrics should be aligned with security objectives, risk appetite, and business goals. Effective metrics allow management to determine whether controls remain appropriate, efficient, and effective in reducing risk to acceptable levels. Reference: CISM Information Security Program Development and Management; security metrics, control monitoring, and performance reporting principles.

NEW QUESTION: 309
Which of the following is the MOST important function of an information security steering committee?
A. Assigning data classifications to organizational assets

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

NEW QUESTION: 310
Which of the following is the PRIMARY responsibility of the information security function when an organization adopts emerging technologies?
Freecram.net
A. Developing security training for the new technologies
B. Designing new security controls
C. Creating an acceptable use policy for the technologies
D. Assessing the potential security risk
Answer: (SHOW ANSWER)
The primary responsibility of the information security function when an organization adopts emerging technologies is to assess the potential security risk, which means identifying and evaluating the threats, vulnerabilities, and impacts that the new technologies may pose to the organization's data, systems, and objectives. Assessing the potential security risk helps the information security function to determine the appropriate security requirements, controls, and measures to mitigate the risk and ensure the safe and secure adoption of the emerging technologies.
References = Performing Risk Assessments of Emerging Technologies, CISM Review Manual 15th Edition Learn more:
1. isaca.org2. isaca.org3. niccs.cisa.gov4. venturebeat.com

NEW QUESTION: 311
An organization would like to invest in a new emerging technology. Which of the following is MOST important for the information security manager to consider when evaluating its impact?
A. Secure configuration
B. Industry peer reviews of the technology
C. Vulnerabilities in the technology
D. Systems compatibility

Answer: (SHOW ANSWER)

NEW QUESTION: 312
Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?
A. Enterprise risk committee
B. Information security steering committee
C. Data privacy officer (DPO)
D. Chief information security officer (CISO)
Answer: (SHOW ANSWER)

NEW QUESTION: 313
How does an organization PRIMARILY benefit from the creation of an information security steering committee?
A. An increased alignment with industry security trends that impact the business
B. An increased alignment of information security with the business
C. An increased focus on information security resource management
D. An increase in information security risk awareness
Answer: (SHOW ANSWER)

NEW QUESTION: 314
An information security manager is concerned with continued security policy violations in a particular business unit despite recent efforts to rectify the situation. What is the BEST course of action?
A. Enforce sanctions on the business unit.
B. Revise the policy to accommodate the business unit.
C. Report the business unit for policy noncompliance.
D. Review the business unit's function against the policy.
Answer: (SHOW ANSWER)
The best course of action is to review the business unit's function against the policy (D). According to CISM governance principles, persistent policy violations often indicate a misalignment between policy requirements and business operations, rather than willful noncompliance. CISM emphasizes that information security policies must be aligned with business objectives, operational realities, and risk appetite to be effective and enforceable. Before escalating to sanctions (A) or reporting noncompliance (C), the information security manager should determine whether the policy is clearly understood, practical to implement, and supported by appropriate standards and procedures. Revising the policy to accommodate violations (B) without analysis weakens governance and may increase risk. By reviewing the business unit's function against the policy, the security manager can identify root causes such as unclear requirements, missing procedures, inadequate training, or legitimate business constraints requiring approved exceptions or compensating controls.

CISM stresses a root-cause and business-aligned approach to governance issues, ensuring that enforcement actions are justified, proportional, and supported by management intent.
References:
ISACA CISM Review Manual, Information Security Governance - policy alignment, enforcement, and exception management ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 315
Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?
A. A capability and maturity assessment
B. Detailed analysis of security program KPIs
C. An information security dashboard
D. An information security risk register
Answer: (SHOW ANSWER)
An information security dashboard is the most effective way to present quarterly reports to the board on the status of the information security program, because it provides a concise, visual, and high-level overview of the key performance indicators (KPIs), metrics, and trends of the information security program. An information security dashboard can help the board to quickly and easily understand the current state, progress, and performance of the information security program, and to identify any gaps, issues, or areas of improvement. An information security dashboard can also help the board to align the information security program with the organization's business goals and strategies, and to support the decision-making and oversight functions of the board.
A capability and maturity assessment is a way of measuring the effectiveness and efficiency of the information security program, and of identifying the strengths and weaknesses of the program. However, a capability and maturity assessment is not the most effective way to present quarterly reports to the board, because it may not provide a clear and timely picture of the status of the information security program, and it may not reflect the changes and dynamics of the information security environment. A capability and maturity assessment is more suitable for periodic or annual reviews, rather than quarterly reports.
A detailed analysis of security program KPIs is a way of evaluating the performance and progress of the information security program, and of determining the extent to which the program meets the predefined objectives and targets. However, a detailed analysis of security program KPIs is not the most effective way to present quarterly reports to the board, because it may be too technical, complex, or lengthy for the board to comprehend and appreciate. A detailed analysis of security program KPIs is more suitable for operational or tactical level reporting, rather than strategic level reporting.
An information security risk register is a tool for recording and tracking the information security risks that affect the organization, and for documenting the risk assessment, treatment, and monitoring activities.

However, an information security risk register is not the most effective way to present quarterly reports to the board, because it may not provide a comprehensive and balanced view of the information security program, and it may not highlight the achievements and benefits of the program. An information security risk register is more suitable for risk management or audit purposes, rather than performance reporting. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 47-48, 59-60, 63-64, 67-68.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1019.
An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

NEW QUESTION: 316
Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?
A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats
Answer: (SHOW ANSWER)
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

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

NEW QUESTION: 317

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

A. Employee training on ransomware

B. A properly tested offline backup system

C. A continual server replication process

D. A properly configured firewall

Answer: (SHOW ANSWER)

The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures.

Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware.

However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable.

A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 318

Which of the following should be done FIRST to determine the impact of a new regulatory requirement for cloud services?

A. Perform a risk assessment

B. Review the information asset inventory

C. Determine the applicability

D. Conduct a gap analysis

Answer: (SHOW ANSWER)

The correct answer is C because before assessing impact, performing a gap analysis, or conducting a risk assessment, the organization must first determine whether the new regulatory requirement applies to its cloud services, data, jurisdictions, customers, industry, and processing activities. Applicability establishes whether the regulation is relevant and which systems,

processes, contracts, business units, or data types are in scope. A risk assessment is important after applicability is confirmed, but performing it too early may waste resources or miss the correct scope. Reviewing the asset inventory may support scoping, but it should follow or support the applicability analysis. A gap analysis compares current practices against requirements, but this cannot be done properly until the organization confirms that the requirement applies and understands its scope. CISM risk management emphasizes identifying legal, regulatory, and contractual obligations as part of risk and compliance management. Therefore, determining applicability is the first step in understanding the impact of a new regulatory requirement. Reference: CISM Information Risk Management; regulatory compliance, cloud risk, applicability analysis, and risk assessment scoping principles.

NEW QUESTION: 319

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: (SHOW ANSWER)

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: 320

Which of the following is the BEST reason to implement an information security architecture?

A. Serve as a post-deployment information security road map.

B. Assess the cost-effectiveness of the integration.

C. Facilitate consistent implementation of security requirements.

D. Fast-track the deployment of information security components.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 321

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

A. Wipe the affected system.

B. Notify internal legal counsel.

C. Notify senior management.

D. Isolate the impacted endpoints.

Answer: (SHOW ANSWER)

Isolating the impacted endpoints is the best course of action for the information security manager after an employee clicked on a link in a phishing email, triggering a ransomware attack because it prevents the ransomware from spreading to other systems or devices on the network, and minimizes the damage or disruption caused by the attack. Wiping the affected system is not a good course of action because it may destroy any evidence or data that could be used for investigation or recovery. Notifying internal legal counsel is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Notifying senior management is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. References: https://www.isaca.org/resources/isaca-journal/issues
/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 322

An information security manager of an e-commerce business is reviewing the results of a business continuity plan review. Which of the following findings should be the MOST immediate concern?

A. The business continuity plan has not been recently tested

B. The cost of a recent recovery test exceeded budget expectations

C. The annual business impact analysis has been delayed

D. The business continuity plan has not been recently audited

Answer: (SHOW ANSWER)

The correct answer is A because an untested business continuity plan creates immediate uncertainty about whether the organization can continue or recover critical operations during a disruption. For an e-commerce business, downtime can quickly affect revenue, customer trust, regulatory obligations, and service availability. Testing validates whether recovery procedures, people, technologies, communications, dependencies, and recovery objectives are realistic and achievable. A recovery test exceeding budget expectations is a concern, but it does not necessarily mean the organization cannot recover. A delayed business impact analysis is important because BIA supports continuity planning, but the immediate operational concern is that the plan has not been validated. A lack of recent audit may reduce assurance, but an audit is not a substitute for testing. In CISM, continuity and recovery capabilities must be tested to confirm readiness and identify weaknesses before a real incident occurs. Therefore, the absence of recent BCP testing is the most immediate concern.
Reference: CISM Information Security Incident Management; business continuity, disaster recovery, plan testing, and operational resilience principles.

NEW QUESTION: 323
Which of the following is the BEST security control to minimize the risk of successful ransomware attacks?
A. Application deny list
B. Web security gateway
C. Host intrusion detection system
D. Application allow list
Answer: (SHOW ANSWER)
The correct answer is D because application allow listing is one of the most effective preventive controls against ransomware execution. Allow listing permits only approved and authorized applications, scripts, or executables to run, thereby reducing the likelihood that malicious ransomware code can execute on endpoints or servers. An application deny list blocks known malicious applications, but it is less effective because attackers can modify filenames, hashes, or code to bypass known deny rules. A web security gateway can help reduce exposure to malicious downloads, phishing links, and compromised websites, but it does not fully prevent ransomware introduced through other channels. A host intrusion detection system may detect suspicious activity, but detection is reactive and may occur after ransomware has already started execution or encryption. CISM risk management principles favor preventive controls where feasible, especially for high- impact threats. Since ransomware success often depends on unauthorized code execution, application allow listing provides stronger protection than the other options.
Reference: CISM Information Risk Management; malware prevention, ransomware risk, endpoint controls, and preventive security control principles.

NEW QUESTION: 324
Which of the following is the BEST indication ofa successful information security culture?
A. Penetration testing is done regularly and findings remediated.

B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.
Answer: (SHOW ANSWER)
The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Culture, page 281.

NEW QUESTION: 325
An organization has decided to implement an Internet of Things (IoT) solution to remain competitive in the market. Which of the following should information security do FIRST?
A. Recalculate risk profile
B. Implement compensating controls
C. Reassess risk tolerance levels
D. Update the security architecture
Answer: (SHOW ANSWER)
When introducing new technologies, the first step is to recalculate the risk profile to identify any new or changed risks.
"The implementation of new technologies should trigger a review of the risk profile to identify and address new exposures."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis*

NEW QUESTION: 326
Which of the following is the PRIMARY purpose of implementing information security standards?
A. To provide management direction with a specific security objective
B. To provide a basis for developing information security policies
C. To provide step-by-step instructions for performing security-related tasks
D. To establish a minimum acceptable security baseline
Answer: (SHOW ANSWER)

The primary purpose of information security standards is to establish a minimum acceptable security baseline (D). In CISM governance, policies define what must be achieved, standards define the mandatory minimum requirements, and procedures provide how-to instructions. Management direction (A) is the role of policies, not standards. Policies are not derived from standards (B); rather, standards support policies. Step-by-step instructions (C) are procedures. Standards ensure consistency, enforceability, and measurable compliance across the organization.
References: ISACA CISM Review Manual (Governance-policy, standards, and procedures hierarchy); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 327
Prior to implementing a bring your own device (BYOD) program, it is MOST important to:
A. select mobile device management (MDM) software.
B. survey employees for requested applications.
C. develop an acceptable use policy.
D. review currently utilized applications.
Answer: (SHOW ANSWER)
Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non- compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.
References = CISM Review Manual, 16th Edition, page 197

NEW QUESTION: 328
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. Reviewing vendor contracts and service level agreements (SLAs)
B. Developing training for end users to familiarize them with the new technology
C. Assessing how peer organizations using the same technologies have been impacted
D. Understanding the impact on existing resources
Answer: (SHOW ANSWER)

NEW QUESTION: 329
Which of the following would be MOST effective in gaining senior management approval of security investments in network infrastructure?
A. Performing penetration tests against the network to demonstrate business vulnerability
B. Highlighting competitor performance regarding network best security practices
C. Demonstrating that targeted security controls tie to business objectives
D. Presenting comparable security implementation estimates from several vendors
Answer: (SHOW ANSWER)

The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives. Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization ' s business objectives, senior management will be more likely to approve the investment.
According to the Certified Information Security Manager (CISM) Study Manual, " To gain senior management ' s approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization. "
While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization
' s business objectives.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

NEW QUESTION: 330

Which of the following MUST be established to maintain an effective information security governance framework?

Freecram.net

A. Security controls automation
B. Defined security metrics
C. Change management processes
D. Security policy provisions
Answer: (SHOW ANSWER)
Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. References:
* https://www.iso.org/standard/74046.html
* https://www.nistf.gov/cyberframework
* https://www.iso.org/standard/27001

NEW QUESTION: 331
Which of the following should be the GREATEST concern for an information security manager when an annual audit reveals the organization's business continuity plan (BCP) has not been reviewed or updated in more than a year?

A. An outdated BCP may result in less efficient recovery if an actual incident occurs.
B. The organization may suffer reputational damage for not following industry best practices.
C. The audit finding may impact the overall risk rating of the organization.
D. The lack of updates to the BCP may result in noncompliance with internal policies.
Answer: (SHOW ANSWER)
A BCP is a document that outlines the processes and procedures to maintain or resume critical business functions and minimize the impact of a disruption on the organization's objectives, customers, and stakeholders. A BCP should be reviewed and updated regularly to reflect the changes in the organization's environment, risks, resources, and requirements. An outdated BCP may result in less efficient recovery if an actual incident occurs, as it may not account for the current situation, dependencies, priorities, or recovery strategies. This may lead to increased downtime, losses, or damages for the organization.
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 Plans

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

NEW QUESTION: 332
Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?
A. Providing training from third-party forensics firms
B. Obtaining industry certifications for the response team
C. Conducting tabletop exercises appropriate for the organization
D. Documenting multiple scenarios for the organization and response steps
Answer: (SHOW ANSWER)
The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.

According to the Certified Information Security Manager (CISM) Study Manual, "Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan." While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

NEW QUESTION: 333
Which of the following is the MOST important consideration when developing key performance indicators (KPIs) for the information security program?
A. Alignment with financial reporting
B. Alignment with business initiatives
C. Alignment with industry frameworks
D. Alignment with risk appetite
Answer: (SHOW ANSWER)
Explore
The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain - Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

NEW QUESTION: 334
Management decisions concerning information security investments will be MOST effective when they are based on:

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

NEW QUESTION: 335
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: 336
In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?
A. Communicate regular reminders of the acceptable use policy
B. Include the topic of prohibited texting in security awareness training

C. Stop providing mobile devices until the organization is able to implement controls
D. Conduct a business impact analysis (BIA) and provide the report to management
Answer: (SHOW ANSWER)
In the absence of technical controls, the best way to reduce unauthorized text messaging is to include the topic of prohibited texting in security awareness training . CISM recognizes that when automated or technical enforcement is unavailable, user behavior must be influenced through targeted awareness and training. Training is stronger than simple reminders because it can explain the policy requirement, business rationale, examples of prohibited behavior, consequences of noncompliance, and proper alternatives. Regular reminders of the acceptable use policy may help reinforce expectations, but they are less effective than structured training. Stopping mobile device use would likely disrupt business and may not be proportionate to the risk. Conducting a BIA is unrelated because the issue is user behavior and policy compliance, not continuity prioritization. CISM emphasizes that awareness and training programs should be tailored to specific roles, technologies, and behaviors. Therefore, incorporating prohibited texting into security awareness training is the best compensating measure when technical controls are not available.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - security awareness and acceptable use ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 337
A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?
A. Automated controls
B. Security policies
C. Guidelines
D. Standards
Answer: (SHOW ANSWER)
Standards are the most important thing to review, as they define the specific and mandatory requirements for setting up new user accounts, such as the naming conventions, access rights, password policies, and expiration dates. Standards help to ensure consistency, security, and compliance across the organization's information systems and users. If the standards are not followed, the organization may face increased risks of unauthorized access, data breaches, or audit failures.
References = CISM Review Manual 2022, page 341; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.32; CISM 2020: IT Security Policies; Information Security Policy, Standards, and Guidelines

NEW QUESTION: 338

Which of the following metrics would BEST demonstrate the success of a newly implemented information security framework?

A. An increase in the number of identified security incidents

B. An increase in the number of compliant business processes

C. A decrease in the number of security audit findings

D. A decrease in the number of security policy exceptions

Answer: B (LEAVE A REPLY)

NEW QUESTION: 339

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: (SHOW ANSWER)

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: 340

The GREATEST benefit of an effective information security awareness program is the organization's ability to:

Freecram.net

A. Meet compliance requirements

B. Reduce security incidents

C. Establish accountability

D. Develop meaningful metrics

Answer: (SHOW ANSWER)

The greatest benefit of an effective awareness program is the reduction of security incidents (B). CISM stresses that awareness aims to change behavior, which directly lowers the likelihood of incidents such as phishing, data leakage, and policy violations. Compliance (A), accountability (C), and metrics (D) are secondary outcomes. The true measure of success is improved risk posture through fewer and less severe incidents.
References: ISACA CISM Review Manual (Program management-security awareness and behavior); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 341
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: 342
An information security manager has become aware that a third-party provider is not in compliance with the statement of work (SOW). Which of the following is the BEST course of action?
A. Notify senior management of the issue.

B. Report the issue to legal personnel.
C. Initiate contract renegotiation.
D. Assess the extent of the issue.
Answer: (SHOW ANSWER)
The first course of action when the information security manager becomes aware that a third-party provider is not in compliance with the SOW is to assess the extent of the issue, which means determining the nature, scope, and impact of the non-compliance on the security of the enterprise's data and systems. The assessment should also identify the root cause of the non-compliance and the possible remediation actions. The assessment will help the information security manager to decide the next steps, such as notifying senior management, reporting the issue to legal personnel, initiating contract renegotiation, or terminating the contract.
References = Ensuring Vendor Compliance and Third-Party Risk Mitigation, A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

NEW QUESTION: 343
IT projects have gone over budget with too many security controls being added post-production. Which of the following would MOST help to ensure that relevant controls are applied to a project?
A. Involving information security at each stage of project management
B. Identifying responsibilities during the project business case analysis
C. Creating a data classification framework and providing it to stakeholders
D. Providing stakeholders with minimum information security requirements
Answer: (SHOW ANSWER)
The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

NEW QUESTION: 344
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?
A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.
Answer: (SHOW ANSWER)

A vulnerability assessment process is a systematic and proactive approach to identify, analyze and prioritize the vulnerabilities in an information system. It helps to reduce the exposure of the system to potential threats and improve the security posture of the organization. By implementing a vulnerability assessment process, the organization can facilitate proactive risk management, which is the PRIMARY benefit of this process.
Proactive risk management is the process of identifying, assessing and mitigating risks before they become incidents or cause significant impact to the organization. Proactive risk management enables the organization to align its security strategy with its business objectives, optimize its security resources and investments, and enhance its resilience and compliance.
A). Threat management is enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Threat management is the process of identifying, analyzing and responding to the threats that may exploit the vulnerabilities in an information system. Threat management is enhanced by implementing a vulnerability assessment process, as it helps to reduce the attack surface and prioritize the most critical threats.
However, threat management is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a reactive rather than proactive approach to risk management.
B). Compliance status is improved. This is a secondary benefit of implementing a vulnerability assessment process. Compliance status is the degree to which an organization adheres to the applicable laws, regulations, standards and policies that govern its information security. Compliance status is improved by implementing a vulnerability assessment process, as it helps to demonstrate the organization's commitment to security best practices and meet the expectations of the stakeholders and regulators. However, compliance status is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a result rather than a driver of risk management.
C). Security metrics are enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Security metrics are the quantitative and qualitative measures that indicate the effectiveness and efficiency of the information security processes and controls. Security metrics are enhanced by implementing a vulnerability assessment process, as it helps to provide objective and reliable data for security monitoring and reporting. However, security metrics are not the PRIMARY benefit of implementing a vulnerability assessment process, as they are a means rather than an end of risk management.
References =
* CISM Review Manual 15th Edition, pages 1-301
* CISM Exam Content Outline2
* Risk Assessment for Technical Vulnerabilities3
* A Step-By-Step Guide to Vulnerability Assessment4

NEW QUESTION: 345
Risk treatment options should PRIMARILY focus on:
A. The criticality of impacted assets
B. Reducing risk to an acceptable level

C. High- and medium-rated risks
D. Inherent and residual risks
Answer: (SHOW ANSWER)
The correct answer is B because the purpose of risk treatment is to bring risk within the organization's acceptable level, based on risk appetite and risk tolerance. Risk treatment may involve mitigating, avoiding, transferring, or accepting risk. The objective is not simply to focus on inherent and residual risk as concepts, but to select and apply treatment options that reduce or manage risk to a level approved by the organization.
Asset criticality is an important input because more critical assets may require stronger controls, but it is not the primary purpose of treatment. High- and medium-rated risks often receive priority, but risk treatment should still be based on business impact, likelihood, cost, risk appetite, and treatment effectiveness. Inherent and residual risk must be understood, but they describe risk before and after controls rather than the main focus of selecting treatment. CISM risk management principles emphasize that management must choose treatment options that align risk with business objectives and acceptable risk levels.
Reference: CISM Information Risk Management; risk treatment, risk appetite, residual risk, and risk response principles.

NEW QUESTION: 346
An organization successfully responded to an information security incident. However, the information security manager learned that some of the steps specified in the incident management procedures were not taken by the response team. What should be the information security manager's FIRST step?
A. Provide additional training to the incident response team.
B. Interview the incident response team.
C. Remove the steps from the incident management procedures.
D. Review the incident management procedures.
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 347
An organization has introduced a new bring your own device (BYOD) program. The security manager has determined that a small number of employees are utilizing free cloud storage

services to store company data through their mobile devices. Which of the following is the MOST effective course of action?

A. Allow the practice to continue temporarily for monitoring purposes.

B. Disable the employees' remote access to company email and data

C. Initiate remote wipe of the devices

D. Assess the business need to provide a secure solution

Answer: (SHOW ANSWER)

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

* https://www.digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing- breach
* https://news.microsoft.com/en-xm/2021/03/18/how-to-have-secure-remote-working-with-a-byod-policy/
* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide- bring-your-own-device-byod

NEW QUESTION: 348

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

A. Business process owner

B. Business continuity coordinator

C. Senior management

D. Information security manager

Answer: (SHOW ANSWER)

The business process owner is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The business process owner has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the business process owner is the best person to calculate the recovery time and cost estimates when performing a business impact analysis (BIA), which is a process of identifying and quantifying the potential losses, damages, or consequences that could result from a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The recovery time and cost estimates are the measures that indicate the time and money that are needed to resume and

restore the normal business operations and functions after the disruption or incident. The recovery time and cost estimates can help to prioritize and protect the critical activities and resources, to allocate the appropriate budget and resources, to implement the necessary controls and measures, and to evaluate the effectiveness and efficiency of the business continuity and disaster recovery plans.
The business continuity coordinator, the senior management, and the information security manager are all important roles in the BIA process, but they are not the best ones to calculate the recovery time and cost estimates. The business continuity coordinator is the person who is responsible for coordinating and facilitating the BIA process, as well as the development, implementation, and maintenance of the business continuity and disaster recovery plans. The business continuity coordinator can help to define and communicate the scope, objectives, and methodology of the BIA, to collect and analyze the data and information from the business process owners and other stakeholders, to report and present the BIA results and recommendations, and to provide feedback and suggestions for improvement and optimization of the BIA and the plans. The senior management is the group of people who have the ultimate authority and accountability for the organization's strategy, direction, and performance. The senior management can help to approve and support the BIA process and the plans, to provide the strategic guidance and vision for the business continuity and disaster recovery, to allocate the necessary budget and resources, to oversee and monitor the BIA and the plans, and to make the final decisions and approvals. The information security manager is the person who is responsible for ensuring the security of the information assets and systems that support the business processes and functions. The information security manager can help to identify and assess the information security risks and issues that could affect the BIA and the plans, to implement and manage the security controls and measures that are needed to protect and recover the information assets and systems, to coordinate and collaborate with the business process owners and other stakeholders on the security aspects of the BIA and the plans, and to provide the security expertise and advice. References = CISM Review Manual 15th Edition, pages 228-2291; CISM Practice Quiz, question 1722

NEW QUESTION: 349
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: (SHOW ANSWER)
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: 350

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?

Freecram.net

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: 351
An internal audit has revealed that a number of information assets have been inappropriately classified. To correct the classifications, the remediation accountability should be assigned to:

A. the business users.
B. the information owners.
C. the system administrators.
D. senior management.
Answer: (SHOW ANSWER)
The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities.
This will improve the efficiency, effectiveness, and consistency of the incident response process.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

NEW QUESTION: 352
An outsourced vendor handles an organization's business-critical data. Which of the following is the MOST effective way for the client organization to obtain assurance of the vendor's security practices?
A. Requiring business continuity plans (BCPs) from the vendor
B. Reviewing recent information security disclosures from the vendor
C. Requiring periodic independent third-party reviews
D. Reviewing the vendor service level agreement (SLA)
Answer: (SHOW ANSWER)
The most effective way to obtain assurance of a vendor's security practices is requiring periodic independent third-party reviews (C). In CISM governance and third-party risk management, independent assurance is the strongest mechanism to validate that security controls are not only documented but also designed appropriately and operating effectively. Third-party reviews (such as SOC reports or independent audits) provide objective evidence and reduce reliance on vendor self-reporting.
Requiring BCPs (A) focuses primarily on availability and resilience, not the overall security posture.
Reviewing security disclosures (B) is reactive and limited to known issues disclosed by the vendor.
Reviewing SLAs (D) confirms contractual expectations but does not validate actual control effectiveness.
CISM emphasizes that governance over outsourced services must include ongoing, independent assurance activities to ensure continued alignment with risk appetite and regulatory obligations.
Periodic independent reviews also support accountability, enable risk-based decision-making, and provide defensible evidence of due diligence to senior management and regulators.
References:

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

NEW QUESTION: 353
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: (SHOW ANSWER)
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: 354
An information security manager learns that business unit leaders are encouraging increased use of social media platforms to reach customers. Which of the following should be done FIRST to help mitigate the risk of confidential information being disclosed by employees on social media?
A. Establish an organization-wide social media policy.
B. Develop sanctions for misuse of social media sites.
C. Monitor social media sites visited by employees.
D. Restrict social media access on corporate devices.
Answer: (SHOW ANSWER)
An organization-wide social media policy is a document that defines the rules and guidelines for using social media platforms within the organization. It covers topics such as who can use social media, what they can post, how they should protect confidential information, and what are the consequences for violating the policy. An organization-wide social media policy helps to mitigate the risk of confidential information being disclosed by employees on social media by providing a clear and consistent framework for managing social media activities12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION: 355
Which of the following risks is an example of risk transfer?
A. Utilizing third-party applications

B. Moving risk ownership to another department
C. Conducting off-site backups
D. Purchasing cybersecurity insurance
Answer: (SHOW ANSWER)
Purchasing cybersecurity insurance is a textbook example of risk transfer - transferring financial risk to a third party (the insurer).
"Risk transfer shifts the impact of a risk to another party, such as through insurance or outsourcing."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*

NEW QUESTION: 356
A startup company deployed several new applications with vulnerabilities into production because security reviews were not conducted. What will BEST help to ensure effective application risk management going forward?
A. Conduct automated scans on applications before deployment.
B. Supplement existing development teams with security engineers.
C. Integrate information security into existing change management.
D. Create a new governance council for application security.
Answer: (SHOW ANSWER)
Integrating information security into existing change management processes ensures that security considerations are included in all application changes and deployments. This addresses the root cause of bypassed security reviews and provides a consistent, repeatable process to manage risk going forward.
"Integrating security into change management ensures that changes to systems and applications undergo appropriate security review and testing prior to implementation, thereby addressing vulnerabilities proactively."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Change Management*

NEW QUESTION: 357
Which of the following provides the BEST indication of the return on information security investment?
A. Increased annualized loss expectancy (ALE)
B. Increased number of reported incidents
C. Reduced annualized loss expectancy (ALE)
D. Decreased number of reported incidents
Answer: (SHOW ANSWER)
A reduction in annualized loss expectancy (ALE) demonstrates that implemented controls have effectively reduced the organization's exposure to risk.
"ALE reduction is a key indicator of the cost-effectiveness of security investments and the improvement of the risk posture."

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

NEW QUESTION: 358
Which of the following should be done FIRST after a ransomware incident has been successfully contained?
A. Restore impacted systems.
B. Conduct forensic analysis.
C. Notify relevant stakeholders.
D. Perform lessons learned.
Answer: (SHOW ANSWER)

NEW QUESTION: 359
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?
A. Document risk acceptances.
B. Revise the organization's security policy.
C. Assess the consequences of noncompliance.
D. Conduct an information security audit.
Answer: (SHOW ANSWER)
Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done. These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the

consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it. References = CISM Review Manual
2023, page 43 1; CISM Practice Quiz 2

NEW QUESTION: 360

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

Freecram.net

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

NEW QUESTION: 361

Which of the following is the PRIMARY role of an information security manager in a software development project?
A. To enhance awareness for secure software design
B. To assess and approve the security application architecture
C. To identify noncompliance in the early design stage
D. To identify software security weaknesses
Answer: (SHOW ANSWER)
The primary role of an information security manager in a software development project is to assess and approve the security application architecture. The security application architecture is the design and structure of the software application that defines how the application components interact with each other and with external systems, and how the application implements the security requirements, principles, and best practices. The information security manager is responsible for ensuring that the security application architecture is aligned with the organization's information security policies, standards, and guidelines, and that it meets the business objectives, functional specifications, and user expectations. The information security manager is also responsible for reviewing and evaluating the security application architecture for its completeness, correctness, consistency, and compliance, and for identifying and resolving any security issues, risks, or gaps. The information security manager is also responsible for approving the security application architecture before the software development project proceeds to the next phase, such as coding, testing, or deployment.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 80, page 742.

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

NEW QUESTION: 362
The manager of a key project has bypassed the standard contractor onboarding process to acquire additional resources for delivering the project on time. Contracts were executed offline, and contractors were provided organizational access without going through the standard due diligence process. Which of the following should be the PRIMARY concern?
A. The contractors may inappropriately outsource the business functions to fourth-party suppliers
B. There are insufficient contractual requirements in place to govern third-party arrangements
C. The project may be delayed further if the incident is reported
D. The contractors may not operate in line with industry benchmarks
Answer: (SHOW ANSWER)
The correct answer is B because bypassing the standard onboarding and due diligence process creates a major third-party risk, especially where contracts were executed offline and access was granted without proper review. The primary concern is that the organization may lack sufficient contractual security, privacy, compliance, audit, service, incident notification, confidentiality, and termination requirements to govern the contractor relationship. Fourth-party outsourcing is possible, but it is only one risk that should normally be controlled through contract terms and due diligence. Further project delay is a business concern, but it should not override security and risk management requirements. Industry benchmarks may be useful, but they are not the main issue. CISM risk management principles require that third-party relationships be governed through due diligence, risk assessment, clearly defined responsibilities, access controls, and enforceable contractual obligations. Granting organizational access without proper contractual and risk controls can expose sensitive information, systems, and business processes to unacceptable risk. Reference: CISM Information Risk Management; third-party risk management, contractor onboarding, due diligence, access governance, and contractual control principles.

NEW QUESTION: 363
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: (SHOW ANSWER)
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: 364
Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?
A. Intrusion detection
B. Log monitoring
C. Patch management
D. Antivirus software
Answer: (SHOW ANSWER)
= Patch management is the process of applying updates to software and hardware systems to fix security vulnerabilities and improve functionality. Patch management is one of the best ways to prevent the exploitation of system vulnerabilities, as it reduces the attack surface and closes the gaps that attackers can exploit. Patch management also helps to ensure compliance with security standards and regulations, and maintain the performance and availability of systems.
Intrusion detection is the process of monitoring network or system activities for signs of malicious or unauthorized behavior. Intrusion detection can help to detect and respond to attacks, but it does not prevent them from happening in the first place. Log monitoring is the process of collecting, analyzing and reviewing log files generated by various systems and applications. Log monitoring can help to identify anomalies, errors and security incidents, but it does not prevent them from occurring. Antivirus software is the program that scans files and systems for viruses, malware and other malicious code. Antivirus software can help to protect systems from infection, but it does not prevent the exploitation of system vulnerabilities that are not related to malware.
Therefore, patch management is the best security process to prevent the exploitation of system vulnerabilities, as it addresses the root cause of the problem and reduces the risk of compromise.
References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 204.

NEW QUESTION: 365
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?
A. The time and location that the breach occurred
B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error
Answer: (SHOW ANSWER)
The underlying reason for the user error is the most important factor to determine during the post-incident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents. References = CISM Review Manual 2023, page
1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

NEW QUESTION: 366
Which of the following is the BEST source of information to support an organization's information security vision and strategy?
A. Enterprise information security architecture
B. Metrics dashboard
C. Capability maturity model
D. Governance policies
Answer: (SHOW ANSWER)

NEW QUESTION: 367
Which of the following is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?
A. To reduce the overall cost of policy development
B. To share responsibility for addressing security breaches
C. To decrease the workload of the IT department
D. To gain acceptance of the policy across the organization
Answer: (SHOW ANSWER)

The main reason to involve stakeholders from various business units is to gain their acceptance and buy-in for the information security policy. The CISM Review Manual underlines that policies are more effective and enforceable when stakeholders understand and agree with them, which also aids in smooth policy implementation across the organization.
Reference:ISACA CISM Review Manual, 16th Edition, Page 45, "Stakeholder Involvement in Policy Development".

NEW QUESTION: 368
Which of the following is a desired outcome of information security governance?
A. Penetration test
B. Improved risk management
C. Business agility
D. A maturity model
Answer: C (LEAVE A REPLY)
Business agility is a desired outcome of information security governance, as it enables the organization to respond quickly and effectively to changing business needs and opportunities, while maintaining a high level of security and risk management. Information security governance provides the strategic direction, policies, standards, and oversight for the information security program, ensuring that it aligns with the organization's business objectives and stakeholder expectations. Information security governance also facilitates the integration of security into the business processes and systems, enhancing the organization's ability to adapt to the dynamic and complex environment. By implementing information security governance, the organization can achieve business agility, as well as other benefits such as improved risk management, compliance, reputation, and value creation. References = CISM Review Manual 15th Edition, page 25.

NEW QUESTION: 369
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: 370

Which of the following metrics provides the BEST evidence of alignment of information security governance with corporate governance?

Freecram.net

A. Average return on investment (ROI) associated with security initiatives

B. Average number of security incidents across business units

C. Mean time to resolution (MTTR) for enterprise-wide security incidents

D. Number of vulnerabilities identified for high-risk information assets

Answer: (SHOW ANSWER)

Average return on investment (ROI) associated with security initiatives is the best metric to provide evidence of alignment of information security governance with corporate governance because it demonstrates the value and benefits of security investments to the organization's strategic goals and objectives. Average number of security incidents across business units is not a good metric because it does not measure the effectiveness or efficiency of security initiatives or their alignment with corporate governance. Mean time to resolution (MTTR) for enterprise-wide security incidents is not a good metric because it does not measure the impact or outcome of security initiatives or their alignment with corporate governance. Number of vulnerabilities identified for high-risk information assets is not a good metric because it does not measure the performance or improvement of security initiatives or their alignment with corporate governance.
References: https://www.
isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security- investments https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the- effectiveness-of-information-security-governance

NEW QUESTION: 371

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: 372

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: 373
A data discovery project uncovers an unclassified process document. Of the following, who is BEST suited to determine the classification?
A. Data custodian
B. Creator of the document
C. Information security manager
D. Security policy author
Answer: (SHOW ANSWER)

NEW QUESTION: 374
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: 375
During the selection of a Software as a Service (SaaS) vendor for a business process, the vendor provides evidence of a globally accepted information security certification. Which of the following is the MOST important consideration?
A. The certification includes industry-recognized security controls.
B. The certification was issued within the last five years.

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

NEW QUESTION: 376
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?
A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.
Answer: (SHOW ANSWER)
Defining information security requirements and processes is the FIRST thing that the information security manager should do to support the initiative of utilizing Software as a Service (SaaS) and selecting a vendor.
This is because information security requirements and processes provide the basis for evaluating and comparing the SaaS vendors and solutions, as well as for ensuring the alignment of the SaaS services with the organization's security objectives, policies, and standards. Information security requirements and processes should include aspects such as data protection, access control, encryption, authentication, authorization, audit, compliance, incident response, disaster recovery, and service level agreements12. Reviewing independent security assessment reports for each vendor (A) is a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Independent security assessment reports can provide valuable information about the security posture, practices, and performance of the SaaS vendors and solutions, such as their compliance with industry standards, frameworks, and regulations, their vulnerability and risk management, and their security testing and auditing results. However, reviewing independent security assessment reports should be done after defining the information security requirements and processes, which can help to determine the scope, criteria, and expectations for the security assessment12. Benchmarking each vendor's services with industry best practices (B) is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Benchmarking each vendor's services with industry best practices can help to measure and compare the quality, performance, and value of the SaaS vendors and solutions, as well as to identify the gaps, strengths, and weaknesses of the

SaaS services. However, benchmarking each vendor's services with industry best practices should be done after defining the information security requirements and processes, which can help to select the relevant and appropriate industry best practices for the SaaS services12. Analyzing the risks and proposing mitigating controls is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Analyzing the risks and proposing mitigating controls can help to identify and evaluate the potential threats, vulnerabilities, and impacts that may affect the security, availability, and reliability of the SaaS vendors and solutions, as well as to recommend and implement the necessary measures to reduce or eliminate the risks. However, analyzing the risks and proposing mitigating controls should be done after defining the information security requirements and processes, which can help to establish the risk appetite, tolerance, and criteria for the SaaS services12. References = 1: CISM Review Manual 15th Edition, page 82-831; 2: How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria - Gartner2

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

NEW QUESTION: 377
Of the following, who is MOST appropriate to own the risk associated with the failure of a privileged access control?
A. Data owner
B. Business owner
C. Information security manager
D. Compliance manager
Answer: (SHOW ANSWER)
The business owner is the most appropriate person to own the risk associated with the failure of a privileged access control because they are ultimately responsible for the protection and use of the information in their business unit1. The data owner is responsible for determining the access rights for specific data sets, but not for the access control mechanisms2. The information security manager is responsible for implementing and enforcing the security policies and standards, but not for owning the risk3. The compliance manager is responsible for ensuring that the organization meets the regulatory requirements, but not for owning the risk3.
References: 1 https://www.cyberark.com/resources/blog/how-do-you-prioritize-risk-for-privileged-access- management 3 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for- privileged-access-management 2

https://security.stackexchange.com/questions/218049/what-is-the-difference- between-data-owner-data-custodian-and-system-owner

NEW QUESTION: 378
Which of the following BEST ensures timely and reliable access to services?
A. Nonrepudiation
B. Authenticity
C. Availability
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)
= According to the CISM Review Manual, availability is the degree to which information and systems are accessible to authorized users in a timely and reliable manner1. Availability ensures that services are delivered to the users as expected and agreed upon. Nonrepudiation is the ability to prove the occurrence of a claimed event or action and its originating entities1. It ensures that the parties involved in a transaction cannot deny their involvement. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication1. It ensures that the identity of a subject or resource is valid. Recovery time objective (RTO) is the maximum acceptable period of time that can elapse before the unavailability of a business function severely impacts the organization1. It is a metric used to measure the recovery capability of a system or service, not a factor that ensures timely and reliable access to services. References = CISM Review Manual, 16th Edition, Chapter 2, Information Risk Management, pages 66-67.

NEW QUESTION: 379
A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?
A. Determine the required security controls for the new solution
B. Review the disaster recovery plans (DRPs) of the providers
C. Obtain audit reports on the service providers' hosting environment
D. Align the roles of the organization's and the service providers' stats.
Answer: (SHOW ANSWER)
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 380

When updating the information security policy to accommodate a new regulation, the information security manager should FIRST:

Freecram.net

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

NEW QUESTION: 381
Which of the following is the PRIMARY objective of the incident management recovery phase?
A. To recover business operation support
B. To perform a lessons-learned review
C. To document actions taken to restore IT systems
D. To bring IT services back online
Answer: (SHOW ANSWER)
The correct answer is D because the recovery phase focuses on restoring affected IT services, systems, and operations after containment and eradication have been completed. The objective is to return services to an operational state in a controlled manner while ensuring that the threat has been removed and systems are stable. Recovering business operation support is related to the broader business continuity goal, but the recovery phase of incident management is primarily concerned with restoring IT services and affected environments. Performing a lessons-learned review usually occurs after recovery, during post-incident review or improvement activities. Documenting restoration actions is important for evidence, accountability, and future analysis, but documentation is not the primary objective of recovery. In CISM incident management, recovery includes restoring systems, validating functionality, monitoring for recurrence, and returning operations to normal. Therefore, the primary objective of the recovery phase is to bring IT services back online safely and effectively.
Reference: CISM Information Security Incident Management; recovery phase, service restoration, post- incident activities, and operational resilience principles.

NEW QUESTION: 382
When implementing a security policy for an organization handling personally identifiable information (PII); the MOST important objective should be:
A. strong encryption

B. regulatory compliance.
C. data availability.
D. security awareness training
Answer: (SHOW ANSWER)
Regulatory compliance is the most important objective when implementing a security policy for an organization handling personally identifiable information (PII) because it helps to ensure that the organization meets the legal and ethical obligations to protect the privacy and security of PII. PII is any information that can be used to identify, contact, or locate an individual, such as name, address, email, phone number, social security number, etc. PII is subject to various laws and regulations in different jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Failing to comply with these regulations can result in fines, lawsuits, reputational damage, or loss of trust. Therefore, regulatory compliance is the correct answer.
References:
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en
https://www.digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or- compromise
https://blog.rsisecurity.com/how-to-make-a-personally-identifiable-information-policy/

NEW QUESTION: 383
Which of the following presents the GREATEST challenge to a large multinational organization using an automated identity and access management (1AM) system?
A. Staff turnover rates that significantly exceed industry averages
B. Large number of applications in the organization
C. Inaccurate workforce data from human resources (HR)
D. Frequent changes to user roles during employment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 384
An organization has recently purchased cybersecurity insurance after the board voiced concern about the potential for a security breach. With this response to the perceived risk, the organization:
A. Has avoided the risk associated with a security breach
B. Can safely reduce its internal security expenditure
C. Remains ultimately accountable for the impact of a breach
D. Has implemented redundant controls against a breach
Answer: (SHOW ANSWER)
Even with cybersecurity insurance, the organization remains ultimately accountable for the impact of a breach (C). Insurance represents risk transfer, not risk elimination or avoidance. CISM clearly states that accountability for risk cannot be transferred; only financial impact may be partially

offset. Insurance does not justify reducing security controls (B) and does not constitute redundant controls (D). Avoidance (A) would require eliminating the risky activity entirely. Management must continue to manage, monitor, and mitigate risk in line with appetite, regardless of insurance coverage.
References: ISACA CISM Review Manual (Risk management-risk response strategies, risk transfer); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 385
Which of the following BEST supports effective and timely incident response?
A. Involving internal and external stakeholders
B. Having a documented incident response plan in place
C. Appointing a forensic incident response specialist
D. Maintaining a SIEM solution
Answer: (SHOW ANSWER)
The correct answer is B because a documented incident response plan provides the structured guidance needed for effective and timely response. The plan defines roles, responsibilities, escalation paths, communication procedures, severity classifications, containment strategies, evidence handling, notification requirements, and recovery coordination. Without a documented plan, response activities may be delayed, inconsistent, duplicated, or incomplete. Involving internal and external stakeholders is important, but stakeholder involvement must be organized through the incident response plan. Appointing a forensic specialist may be necessary for certain investigations, but not every incident requires forensic expertise. A SIEM solution is useful for monitoring and detection, but technology alone does not ensure that people know how to respond. CISM incident management principles emphasize preparation, documented procedures, communication, role clarity, and repeatable response processes. A documented plan enables responders to act quickly and consistently under pressure. Therefore, having a documented incident response plan in place best supports effective and timely incident response.
Reference: CISM Information Security Incident Management; incident response planning, documentation, escalation, communication, and response readiness principles.

NEW QUESTION: 386
Which of the following is MOST important to include in an information security policy?
A. Baselines
B. Maturity levels
C. Best practices
D. Management objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 387
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: (SHOW ANSWER)
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: 388
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: 389
Which of the following is established during the preparation phase of an incident response plan?
A. Stakeholder communication plan
B. Chain of custody procedures
C. Recovery time objectives (RTOs)
D. Mean time to respond (MTTR)
Answer: (SHOW ANSWER)

NEW QUESTION: 390
Which of the following has the MOST influence on the inherent risk of an information asset?
A. Risk tolerance
B. Net present value (NPV)
C. Return on investment (ROI)
D. Business criticality
Answer: (SHOW ANSWER)
Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes. References = CISM Review Manual,
16th Edition, page 971
Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

NEW QUESTION: 391

The results of a risk assessment for a potential network reconfiguration reveal a high likelihood of sensitive data being compromised. What is the information security manager's BEST course of action?

A. Recommend additional network segmentation.

B. Seek an independent opinion to confirm the findings.

C. Determine alignment with existing regulations.

D. Report findings to key stakeholders.

Answer: (SHOW ANSWER)

The information security manager's best course of action is to report the findings of the risk assessment to the key stakeholders, such as senior management, business owners, and regulators. This will ensure that the stakeholders are aware of the potential impact of the risk and can make informed decisions on how to address it. The other options are possible actions to take after reporting the findings, but they are not the best course of action in this scenario.

References = CISM Domain 2: Information Risk Management (IRM) [2022 update] (section: Information Risk Response) and CISM ITEM DEVELOPMENT GUIDE - ISACA (page 6, item example 2)

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

NEW QUESTION: 392

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

A. Lack of availability

B. Lack of accountability

C. Improper authorization

D. Inadequate authentication

Answer: (SHOW ANSWER)

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

options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. References:
https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam
https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices
https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

NEW QUESTION: 393
Which of the following is the MOST important consideration when determining which type of failover site to employ?
A. Reciprocal agreements
B. Disaster recovery test results
C. Recovery time objectives (RTOs)
D. Data retention requirements
Answer: (SHOW ANSWER)
The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources. Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

NEW QUESTION: 394

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

NEW QUESTION: 395
Which of the following is the MOST important consideration when attempting to create a security-focused culture?
A. Current security strategy benchmarks against peer organizations
B. The regional rules and legislation regarding information security
C. The current security awareness level of the employees
D. The organization's existing security policies, procedures, and frameworks
Answer: (SHOW ANSWER)
The most important consideration is the current security awareness level of employees (C). CISM emphasizes that culture change must start from an understanding of current behaviors, attitudes, and knowledge gaps.
Benchmarking (A), regulations (B), and formal frameworks (D) provide structure, but culture is driven by people. Tailoring initiatives to the existing awareness level increases adoption and effectiveness, leading to sustainable risk reduction.
References: ISACA CISM Review Manual (Program management-security culture development); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 396

Which of the following would pose the GREATEST risk to the preparedness of an incident response team?

A. Lack of formal incident response scenarios

B. A change in information security management

C. Outdated incident response plans

D. New attack vectors used by hackers

Answer: (SHOW ANSWER)

The correct answer is A because formal incident response scenarios are essential for preparing the incident response team to recognize, coordinate, escalate, contain, and recover from realistic incident situations.

Preparedness is built through planning, exercises, role clarity, communications testing, and scenario-based practice. Without formal scenarios, the team may not be able to test whether procedures are practical, whether roles are understood, or whether communications and escalation paths work under pressure. A change in information security management may affect leadership, but it does not automatically reduce team preparedness if processes remain sound. Outdated incident response plans are a serious concern; however, the question focuses on team preparedness, and scenario-based training is a direct mechanism for preparing the team. New attack vectors are expected in a changing threat environment, but a well-prepared team with practiced response scenarios can adapt more effectively. CISM emphasizes testing, exercises, and lessons learned as key elements of incident response capability.

Reference: CISM Information Security Incident Management; incident response preparedness, scenario testing, exercises, and team readiness principles.

NEW QUESTION: 397

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. Identify the data to be hosted.

C. Perform a risk assessment.

D. Analyze the business requirements.

Answer: (SHOW ANSWER)

NEW QUESTION: 398

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

A. Replace the control

B. Check for defense in depth

C. Assess the control state

D. Report the failure to management

Answer: (SHOW ANSWER)

The best first step is to assess the control state to determine why it is ineffective and whether adjustments, replacements, or compensating controls are needed.
"Regularly assess the effectiveness of security controls to ensure they are providing the intended level of protection."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Control Monitoring and Assessment* ISACA practice questions stress that assessing the control state comes before taking further action.

NEW QUESTION: 399
Which of the following is MOST important to ensuring that incident management plans are executed effectively?
A. A reputable managed security services provider has been engaged.
B. The incident response team has the appropriate training.
C. An incident response maturity assessment has been conducted.
D. Management support and approval has been obtained.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 400
Which of the following is the BEST indication of an effective disaster recovery planning process?
A. Hot sites are required for any declared disaster.
B. Recovery time objectives (RTOs) are shorter than recovery point objectives (RPOs).
C. Post-incident reviews are conducted after each event.
D. Chain of custody is maintained throughout the disaster recovery process.
Answer: (SHOW ANSWER)

NEW QUESTION: 401
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:
A. service level agreements (SLAs)
B. security requirements for the process being outsourced.
C. risk-reporting methodologies.
D. security metrics
Answer: (SHOW ANSWER)
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus primarily on defining security requirements for the process being outsourced.
Security requirements are the specifications of what needs to be done to protect the information assets from unauthorized access, use, disclosure, modification, or destruction. Security requirements should be aligned with the organization's risk appetite and business objectives, and

should cover both technical and organizational aspects of the service delivery. Security requirements should also be clear, concise, measurable, achievable, realistic, and testable.
References = CISM Review Manual (Digital Version), Chapter
3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information.
They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are essential to protect the information assets of the organization and to establish a clear and 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: 402
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: (SHOW ANSWER)
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: 403
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: 404
Which of the following should be the FIRST step in developing an information security strategy?
A. Determine acceptable levels of information security risk
B. Create a roadmap to identify security baselines and controls
C. Perform a gap analysis based on the current state
D. Identify key stakeholders to champion information security
Answer: (SHOW ANSWER)
The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them. Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

NEW QUESTION: 405
Which of the following is the MOST likely reason for a vulnerability scanner to return incomplete results?
A. Unauthenticated vulnerability scans are being performed.
B. Scan results are not ingested into a security information and event management (SIEM) tool.
C. Host names have not been fully enumerated.
D. Zero-day vulnerability signatures have not been ingested.
Answer: (SHOW ANSWER)

NEW QUESTION: 406

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

A. The plan is based on risk assessment results.

B. The response team is trained on the plan

C. The plan is based on industry best practice.

D. The incident response plan aligns with the IT disaster recovery plan (DRP).

Answer: (SHOW ANSWER)

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

The scope and objectives of the plan The roles and responsibilities of each team member The communication and escalation protocols The incident classification and prioritization criteria The incident response procedures and tools The incident documentation and reporting requirements The incident review and improvement processes By training the response team on the plan, the organization can ensure that the team members are prepared and confident to handle any security incidents that may occur, and that they can perform their tasks efficiently and consistently. The other options are not the best way to facilitate the effective execution of an incident response plan, although they may be some steps or outcomes of the process.

The plan being based on risk assessment results is a desirable practice, as it ensures that the plan is aligned with the organization's risk profile and addresses the most relevant and likely threats and vulnerabilities.

However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The plan being based on industry best practice is a desirable practice, as it ensures that the plan follows established standards and guidelines for incident

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

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

NEW QUESTION: 407
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 in the business continuity plan (BCP) to manage this requirement?
A. Maximum tolerable downtime (MTD)
B. Service level agreement (SLA)
C. Recovery point objective (RPO)
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)
The Recovery Time Objective (RTO) defines the maximum acceptable downtime for a business function or system following a disruption. If the organization requires recovery in 30 minutes, that is the system's RTO.
This metric guides the selection of technologies, staffing, and procedures needed to meet recovery expectations.
"RTO defines the target time set for the recovery of IT and business activities after a disruption. It is a key BCP design parameter."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery Planning*

NEW QUESTION: 408
An organization's information security team presented the risk register at a recent information security steering committee meeting. Which of the following should be of MOST concern to the committee?
A. No owners were identified for some risks.
B. Business applications had the highest number of risks.

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

NEW QUESTION: 409
Which of the following is PRIMARILY determined by asset classification?
A. Insurance coverage required for assets
B. Level of protection required for assets
C. Priority for asset replacement
D. Replacement cost of assets
Answer: (SHOW ANSWER)
Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. References = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

NEW QUESTION: 410
Which of the following is the PRIMARY impact of organizational culture on the effectiveness of an information security program?
Freecram.net
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: 411
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?
A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule
Answer: (SHOW ANSWER)
The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

NEW QUESTION: 412
Which of the following provides the BEST evidence that a newly implemented security awareness program has been effective?
A. Senior management supports funding for ongoing awareness training.
B. Employees from each department have completed the required training.
C. There have been no reported successful phishing attempts since the training started.
D. There has been an increase in the number of phishing attempts reported.
Answer: (SHOW ANSWER)

NEW QUESTION: 413

Of the following, who is responsible for ensuring security controls are aligned with business objectives and regulatory requirements?

A. Risk owner

B. Control owner

C. Compliance manager

D. Control assessor

Answer: (SHOW ANSWER)

The correct answer is A because the risk owner is accountable for managing risk associated with a business process, asset, or activity. Since risks arise in a business context, the risk owner must ensure that selected controls align with business objectives, risk appetite, and applicable regulatory requirements. Control owners are responsible for implementing, operating, and maintaining specific controls, but they do not own the business risk itself. Compliance managers help interpret and monitor compliance requirements, but they are not usually accountable for business risk treatment decisions. Control assessors evaluate whether controls are designed and operating effectively, but they do not own the risk or determine business alignment. CISM places strong emphasis on business ownership of information risk. Information security managers support and advise, but accountability for risk remains with the business or risk owner. Therefore, the risk owner is responsible for ensuring that controls appropriately support business objectives and regulatory obligations.

Reference: CISM Information Risk Management; risk ownership, accountability, control alignment, and regulatory compliance principles.

NEW QUESTION: 414

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

A. Periodically change risk awareness messages.

B. Periodically test compliance with security controls.

C. Ensure that threats are documented and communicated in a timely manner.

D. Establish a channel for staff to report risks.

Answer: (SHOW ANSWER)

NEW QUESTION: 415

Which of the following is the PRIMARY objective of a cyber resilience strategy?

A. Employee awareness

B. Business continuity

C. Executive support

D. Regulatory compliance

Answer: (SHOW ANSWER)

The primary objective of a cyber resilience strategy is business continuity (B). In CISM, cyber resilience is defined as the organization's ability to prepare for, respond to, recover from, and adapt to adverse cyber events while continuing to deliver critical business services. The focus is

not on preventing all incidents- which is unrealistic-but on ensuring that essential operations can continue or be restored within acceptable timeframes despite cyber disruptions.
Employee awareness (A) and executive support (C) are important enablers of resilience, but they are means, not the ultimate objective. Regulatory compliance (D) is a governance requirement, but compliance alone does not guarantee operational resilience. CISM emphasizes that resilience strategies are driven by business impact analysis (BIA) results, recovery objectives, and tolerance for disruption, all of which directly support continuity of critical services.
A cyber resilience strategy integrates incident response, disaster recovery, backup, redundancy, and crisis management to minimize operational impact. Therefore, ensuring business continuity and operational resilience is the core objective against which cyber resilience effectiveness is measured.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - cyber resilience and business continuity ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

NEW QUESTION: 416
Management would like to understand the risk associated with engaging an Infrastructure-as-a-Service (IaaS) provider compared to hosting internally. Which of the following would provide the BEST method of comparing risk scenarios?
A. Mapping risk scenarios according to sensitivity of data
B. Reviewing mitigating and compensating controls for each risk scenario
C. Mapping the risk scenarios by likelihood and impact on a chart
D. Performing a risk assessment on the IaaS provider
Answer: (SHOW ANSWER)
Mapping the risk scenarios by likelihood and impact on a chart is the best method of comparing risk scenarios, as it helps to visualize and prioritize the different types and levels of risks associated with each option. A chart can also facilitate the communication and decision-making process by showing the trade-offs and benefits of each option. A chart can be based on qualitative or quantitative data, depending on the availability and accuracy of the information.
References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; A risk assessment model for selecting cloud service providers; Security best practices for IaaS workloads in Azure

NEW QUESTION: 417
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: 418

An organization has determined that fixing a security vulnerability in a critical application is too costly to be feasible, but the impact is material to the business. Which of the following is the MOST appropriate risk treatment?

A. Accept the risk associated with continued use of the application.

B. Implement compensating controls for the application.

C. Discontinue using the application.

D. Purchase cybersecurity insurance.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 419

Which of the following BEST illustrates residual risk within an organization?

A. Balanced scorecard

B. Risk management framework

C. Heat map

D. Business impact analysis (BIA)

Answer: C (LEAVE A REPLY)

NEW QUESTION: 420

Of the following, who is in the BEST position to evaluate business impacts?

A. Senior management

B. Information security manager

C. IT manager

D. Process manager

Answer: (SHOW ANSWER)

The process manager is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The process manager has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the process manager is in the best position to evaluate the business impacts of a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The process

manager can identify and quantify the potential losses, damages, or consequences that could result from the disruption or incident, such as revenue loss, customer dissatisfaction, regulatory non-compliance, reputational harm, or legal liability. The process manager can also provide input and feedback to the information security manager and the senior management on the business continuity and disaster recovery plans, the risk assessment and treatment, and the security controls and measures that are needed to protect and recover the business processes and functions. References = CISM Review Manual 15th Edition, page 2301; CISM Practice Quiz, question 1302

NEW QUESTION: 421
Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?
A. Requiring an external security audit of the IT service provider
B. Requiring regular reporting from the IT service provider
C. Defining information security requirements with internal IT
D. Defining the business recovery plan with the IT service provider
Answer: B (LEAVE A REPLY)
Requiring regular reporting from the IT service provider is the best way to ensure compliance with the organization's information security requirements, as it allows the organization to monitor the performance, security incidents, service levels, and compliance status of the IT service provider. Reporting also helps to identify any gaps or issues that need to be addressed or resolved. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

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

NEW QUESTION: 422
Which of the following is the MOST effective way to ensure information security policies are understood?
A. Implement a whistle-blower program.
B. Provide regular security awareness training.
C. Include security responsibilities in job descriptions.
D. Document security procedures.
Answer: (SHOW ANSWER)

Security awareness training is the most effective way to ensure information security policies are understood, as it educates employees on the purpose, content and importance of the policies, and how to comply with them. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

NEW QUESTION: 423
An organization is in the process of acquiring a new company. Which of the following is the FIRST step to determine how to protect newly acquired data assets prior to integration?
A. Inventory information assets
B. Include security requirements in the contract
C. Assess security controls
D. Review data architecture
Answer: (SHOW ANSWER)
The correct answer is A because the organization must first identify and inventory the newly acquired information assets before determining how to protect them. Without knowing what data assets exist, where they are located, who owns them, how they are used, and what sensitivity or criticality they have, the organization cannot select appropriate controls. Including security requirements in the contract is important during acquisition planning, but the question asks how to protect newly acquired data assets prior to integration. Assessing controls is necessary, but it should be based on a clear understanding of the assets being protected. Reviewing data architecture is useful, but it is also dependent on first identifying the assets and their locations. CISM risk management emphasizes asset identification, ownership, classification, and risk assessment as foundational steps in protecting information. An asset inventory enables classification, impact analysis, access review, control selection, and integration planning. Therefore, inventorying information assets is the correct first step.
Reference: CISM Information Risk Management; asset inventory, information classification, acquisition risk, and data protection planning principles.

NEW QUESTION: 424
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: (SHOW ANSWER)
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: 425
A small organization needs to use a solution that is out of support in order to meet business objectives. Which of the following is the information security manager's BEST course of action to manage the associated risk?
A. Run periodic vulnerability scans
B. Advise business units to change the system
C. Recommend that the risk be accepted by senior leadership
D. Implement compensating security controls
Answer: (SHOW ANSWER)
The correct answer is C because the use of an unsupported solution creates risk that may not be fully remediated, especially if patches, vendor fixes, or official support are no longer available. Since the organization needs the solution to meet business objectives, the information security manager should ensure that the risk is formally understood and accepted by the appropriate level of senior leadership or business ownership. The security manager can recommend controls and provide risk information, but should not personally accept business risk. Vulnerability scans may help identify weaknesses, but they do not resolve the fundamental issue of unsupported technology. Advising the business to change the system may not be practical if the system is required for business objectives. Compensating controls may reduce risk and should be considered, but residual risk may remain and must be accepted by authorized leadership. CISM emphasizes that risk acceptance is a business decision and must be made by accountable management.
Reference: CISM Information Risk Management; unsupported systems, risk acceptance, compensating controls, senior management accountability, and residual risk principles.

NEW QUESTION: 426
An information security manager believes that information has been classified inappropriately, = the risk of a breach. Which of the following is the information security manager's BEST action?
A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.

D. Complete a risk assessment and refer the results to the data owners.

Answer: (SHOW ANSWER)

= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.

If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach, as well as the cost and benefit of implementing additional security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.

The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security manager. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701; CISM Online Review Course, Domain 3:

Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

NEW QUESTION: 427
Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?
A. Include security requirements in the contract.
B. Update the risk register.
C. Consult with the business owner.
D. Restrict application network access temporarily.
Answer: (SHOW ANSWER)
Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: "The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications." CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third- party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk." Best Practices to Manage Risks in the Cloud - ISACA: "The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance."

NEW QUESTION: 428
When an organization experiences a disruptive event, the business continuity plan (BCP) should be triggered PRIMARILY based on:
A. expected duration of outage.
B. management direction.
C. type of security incident.
D. the root cause of the event.
Answer: (SHOW ANSWER)

The expected duration of outage is the primary factor that should trigger the BCP because it indicates how long the organization can tolerate the disruption of its critical business processes and functions before it causes unacceptable consequences. The expected duration of outage is determined by the recovery time objectives (RTOs) that are defined for each critical business process and function based on the business impact analysis (BIA). The BCP should be triggered when the expected duration of outage exceeds or is likely to exceed the RTOs.
References: The CISM Review Manual 2023 defines RTO as "the maximum acceptable time that a service can be unavailable or disrupted before it causes unacceptable consequences" and states that "the RTO is determined based on the impact of service interruption on the enterprise's business processes, reputation, customers, and stakeholders" (p. 189). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Expected duration of outage is the correct answer because it is the primary factor that should trigger the BCP, as it reflects the maximum time that the organization can afford to lose its critical business processes and functions without causing unacceptable consequences" (p. 96). Additionally, the article Invoking your business continuity plan: five triggers, six decision points from the ITWeb website states that "the expected duration of outage is the most important consideration when deciding to invoke the BCP, as it indicates how long the organization can sustain the disruption before it impacts its business objectives, operations, reputation, and legal obligations" (p. 2)

NEW QUESTION: 429
Embedding security responsibilities into job descriptions is important PRIMARILY because it:
A. supports access management.
B. simplifies development of the security awareness program.
C. aligns security to the human resources (HR) function.
D. strengthens employee accountability.
Answer: (SHOW ANSWER)
Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

NEW QUESTION: 430

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:

Freecram.net

A. review access rights as the acquisition integration occurs.

B. perform a risk assessment of the access rights.

C. escalate concerns for conflicting access rights to management.

D. implement consistent access control standards.

Answer: (SHOW ANSWER)

Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. References: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful post-merger integration

NEW QUESTION: 431

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: 432
When collecting admissible evidence, which of the following is the MOST important requirement?
A. Need to know
B. Preserving audit logs
C. Due diligence
D. Chain of custody
Answer: (SHOW ANSWER)
Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved.
Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. References = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

NEW QUESTION: 433
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: 434
Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?
A. Conduct a risk assessment.
B. Document disaster recovery procedures.
C. Identify business requirements.
D. Perform a business impact analysis (BIA).
Answer: (SHOW ANSWER)
The business impact analysis (BIA) is the foundational step in disaster recovery planning. The CISM Review Manual states that BIA should be performed first to determine critical business functions, recovery priorities, and the impact of disruptions. Risk assessments and documentation follow after the BIA.
Reference:ISACA CISM Review Manual, 16th Edition, Page 237-238, "Business Impact Analysis (BIA) in DRP Development".

NEW QUESTION: 435
An incident response team has been alerted to suspicious communications between an end user's workstation and a possibly infected external server. Which of the following should be done NEXT?
A. Reinstall the operating system of the end user's workstation
B. Analyze and validate the event
C. Request an IP address block
D. Isolate the end user's workstation and the external server
Answer: (SHOW ANSWER)
The correct answer is B because the next step after receiving an alert is to analyze and validate the event to determine whether it is a true incident, a false positive, or benign activity. Incident response should follow a structured process: detection, validation, classification, prioritization, containment, eradication, recovery, and lessons learned. Reinstalling the operating system is premature and may destroy evidence needed for analysis.
Requesting an IP address block may be appropriate later if the external server is confirmed to be malicious, but blocking without validation can disrupt legitimate business communication. Isolating the workstation may become necessary if compromise is confirmed or strongly suspected, but the question asks what should be done next after an alert. CISM incident management principles require events to be validated before full incident response actions are taken. Proper analysis ensures that response actions are proportionate, evidence is preserved, and business disruption is minimized. Therefore, analyzing and validating the event is the best next step.
Reference: CISM Information Security Incident Management; event validation, incident identification, analysis, classification, and response process principles.

NEW QUESTION: 436

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: (SHOW ANSWER)

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

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

NEW QUESTION: 437

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: 438
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: 439
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:
A. baseline security controls.
B. benchmarking security metrics.
C. security objectives.
D. cost-benefit analyses.
Answer: (SHOW ANSWER)
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address security objectives, which are derived from the business objectives and the risk assessment. Security objectives define the desired level of protection for the system and its data, and guide the selection of security controls in later phases. Baseline security controls are predefined sets of security requirements that apply to common types of systems or environments. Benchmarking security metrics is a process of comparing the performance of security processes or controls against a standard or best practice. Cost-benefit analyses are used to evaluate the feasibility and effectiveness of security controls, and are usually performed in the acquisition/development phase or the implementation phase of the SDLC. References = CISM Review Manual, 16th Edition, page 1021; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 772 Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 440
Which of the following would be MOST important to include in communications to customers impacted by an information security incident?
Freecram.net
A. Details of the type of data exposed
B. Identities of the attackers

C. Costs of the incident to the organization
D. Technical information related to the incident
Answer: (SHOW ANSWER)
The most important information to include in communications to impacted customers is the details of the type of data exposed (A). From a CISM incident management and governance perspective, customer communications must focus on information that enables affected individuals to understand their personal risk and take appropriate protective actions. Knowing what type of data was exposed (e.g., personal identifiers, financial data, credentials, health information) allows customers to assess potential impact, such as identity theft or fraud, and to take timely mitigation steps.
Identities of attackers (B) are often unknown, sensitive, or irrelevant to customers' immediate needs. Costs to the organization (C) are internal matters and do not help customers protect themselves. Technical details (D) may cause confusion, expose additional security information, or create legal and reputational risk without providing practical value to customers.
CISM emphasizes that incident communications should be clear, accurate, relevant, and audience-focused, while also supporting legal, regulatory, and privacy obligations.
Communicating the type of data exposed is central to transparency, trust, and compliance with breach notification requirements.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident communication and stakeholder notification ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 441
Which of the following BEST conveys minimum information security requirements to an organization in alignment with policies?
A. Standards
B. Procedures
C. Regulations
D. Baselines
Answer: A (LEAVE A REPLY)
Standards (A) best convey minimum information security requirements in alignment with organizational policies. In CISM governance, policies define management's intent and direction at a high level, while standards translate that intent into mandatory, enforceable minimum requirements that must be met across the organization. Standards ensure consistency and provide a clear benchmark against which compliance can be measured.
Procedures (B) describe how to perform specific tasks and are operational in nature; they are derived from standards and policies, not used to define minimum requirements. Regulations (C) are external mandates imposed by laws or regulatory bodies and are not internally defined mechanisms for conveying organizational security requirements. Baselines (D) typically represent

a starting configuration or reference point for systems, often derived from standards, but they do not formally communicate organizational requirements on their own.
CISM clearly defines the hierarchy as policy # standards # procedures/guidelines, where standards play the critical role of establishing the minimum acceptable level of security needed to support governance objectives and ensure policy enforcement throughout the enterprise.
References:
ISACA CISM Review Manual, Information Security Governance - policy, standards, and procedures hierarchy ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 442
Which type of recovery site is MOST reliable and can support stringent recovery requirements?
A. Cold site
B. Warm site
C. Hot site
D. Mobile site
Answer: (SHOW ANSWER)
A hot site is the most reliable type of recovery site and can support stringent recovery requirements because it is a fully operational facility that mirrors the primary production center. A hot site has all the hardware, software, data, network, and personnel ready to resume the critical business functions within minutes of a disruptive event. A hot site also has backup power, security, and communication systems to ensure the continuity of operations.
References: The CISM Review Manual 2023 defines a hot site as "a fully operational facility that mirrors the primary production center" and states that "a hot site can support stringent recovery requirements and provide the shortest recovery time" (p. 190). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A hot site is the correct answer because it is the most reliable type of recovery site and can support stringent recovery requirements, as it is a fully operational facility that mirrors the primary production center and can resume the critical business functions within minutes of a disruptive event" (p. 96). Additionally, the web search result 1 states that "the recovery site can be hot, warm, cold or mobile. Hot sites are facilities that mirror the primary production center" and that "hot sites are the most reliable and can support stringent recovery requirements" (p. 1).

NEW QUESTION: 443
Which of the following provides the BEST evidence that a newly implemented security awareness program has been effective?
A. Employees from each department have completed the required training.
B. There have been no reported successful phishing attempts since the training started.
C. Senior management supports funding for ongoing awareness training.
D. There has been an increase in the number of phishing attempts reported.
Answer: (SHOW ANSWER)

NEW QUESTION: 444
During which phase of a security event should an incident response team be INITIALLY engaged?
A. Preparation
B. Eradication
C. Identification
D. Recovery
Answer: (SHOW ANSWER)
The correct answer is C because the incident response team should be initially engaged when a security event is identified as potentially requiring investigation, validation, classification, or escalation. The identification phase involves detecting, reporting, analyzing, and determining whether an event is actually an incident. Early engagement of the incident response team helps ensure the event is validated, categorized, prioritized, and handled according to the incident response plan. Preparation is an important phase in the incident management life cycle, but it occurs before a specific security event and involves planning, training, tools, and readiness. Eradication occurs after the incident is confirmed and containment activities have begun. Recovery occurs after the threat has been removed and services are being restored. CISM emphasizes timely detection, identification, classification, escalation, and response to reduce business impact. Since the question asks when the team should be engaged during a security event, the best answer is the identification phase.
Reference: CISM Information Security Incident Management; incident identification, validation, escalation, classification, and response life cycle principles.

NEW QUESTION: 445
When mitigation is the chosen risk treatment, which of the following roles is responsible for effective implementation of the chosen treatment?
A. Risk owner
B. Control owner
C. Business system owner
D. Application owner
Answer: (SHOW ANSWER)
The control owner is the individual accountable for implementing and managing specific controls that mitigate risks. While the risk owner is responsible for the overall risk and decision-making, it is the control owner who ensures the selected mitigation is effectively implemented and maintained.
"The control owner is responsible for ensuring that the control is properly designed, implemented, and operating effectively."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment
ISACA practice questions stress this distinction: the control owner is tasked with the execution of mitigation strategies.

NEW QUESTION: 446
Which of the following is the MOST effective way to increase security awareness in an organization?
A. Include information security requirements in job descriptions.
B. Conduct periodic simulated phishing exercises.
C. Implement regularly scheduled information security audits.
D. Require signed acknowledgment of information security policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 447
After a server has been attacked, which of the following is the BEST course of action?
A. Initiate incident response.
B. Review vulnerability assessment.
C. Conduct a security audit.
D. Isolate the system.
Answer: (SHOW ANSWER)
Initiating incident response is the best course of action after a server has been attacked because it activates the incident response plan or process, which defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Reviewing vulnerability assessment is not a good course of action because it does not address the current attack or its impact, but rather evaluates the potential weaknesses or exposures of the server. Conducting a security audit is not a good course of action because it does not address the current attack or its impact, but rather verifies and validates the compliance or performance of the server's security controls or systems. Isolating the system is not a good course of action because it does not address the current attack or its impact, but rather stops or limits any communication or interaction with the server. 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: 448
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?
A. Patch management files
B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs
Answer: (SHOW ANSWER)
Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files

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

NEW QUESTION: 449
In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?
A. Data encryption
B. Access to the hardware
C. Compressed customer data
D. Non-standard event logs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 450
Which of the following is MOST important to complete during the recovery phase of an incident response process before bringing affected systems back online?
Freedam.net
A. Test and verify that compromisedsystems are clean.
B. Document recovery steps for senior management reporting.
C. Record and close security incident tickets.
D. Capture and preserve forensic images of affected systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 451
Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?
A. Implement mitigating actions immediately.
B. Invoke the incident response plan.
C. Inform senior management of the breach.
D. Validate the breach.
Answer: (SHOW ANSWER)
The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions.

Invoking the incident response plan or informing management comes after the breach is validated.
Reference:ISACA CISM Review Manual, 16th Edition, Page 280, "Incident Detection and Validation".

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

NEW QUESTION: 452
To align with the principles of Zero Trust, which of the following is the MOST important course of action when engaging with external parties?
A. Requiring external parties to use a specific type of encryption for data at rest and in transit
B. Insisting on regular comprehensive audits of external parties' access management practices
C. Ensuring contracts with external parties mandate continuous verification and least privilege access
D. Mandating that external parties provide annual security training to their employees
Answer: (SHOW ANSWER)
The most important action aligned with Zero Trust principles is ensuring contracts with external parties mandate continuous verification and least privilege access . Zero Trust is based on the principle of "never trust, always verify," requiring ongoing validation of identity, device posture, access context, and authorization. It also requires limiting access to the minimum necessary for the task. Encryption, audits, and annual training are valuable supporting controls, but they do not capture the core operating model of Zero Trust as directly as continuous verification and least privilege. When engaging external parties, contractual requirements are essential because they create enforceable obligations for how access to organizational systems and data must be managed. CISM governance principles emphasize that third-party access should be controlled through documented requirements, accountability, monitoring, and risk-based oversight. Therefore, the best answer is mandating continuous verification and least privilege access in contracts, because this embeds Zero Trust expectations into third-party governance and access management.
References:
ISACA CISM Review Manual , Information Security Governance - third-party access control and security requirements ISACA CISM Exam Content Outline , Domain 2: Information Security Governance

NEW QUESTION: 453
Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?
A. Implement compensating controls to mitigate the noncompliance
B. Validate the noncompliance
C. Include the noncompliance in the risk register
D. Report the noncompliance to senior management
Answer: (SHOW ANSWER)

NEW QUESTION: 454
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: (SHOW ANSWER)
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: 455
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: 456
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: (SHOW ANSWER)
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: 457
Which of the following is the BEST way for the organization to ensure server backups at a warm site are properly maintained and usable during a disaster?
A. Review the backup media storage facilities at the warm site
B. Have duplicate equipment available at the warm site
C. Use the equipment at the warm site facility to read the backups
D. Inspect the facility and inventory the backups on a quarterly basis
Answer: (SHOW ANSWER)
The best way to ensure that backups at a warm site are properly maintained and usable during a disaster is to use the equipment at the warm site facility to read the backups . CISM emphasizes that backup and recovery capabilities must be tested, not merely documented or inspected. Reading the backups using warm- site equipment validates both the backup media and compatibility with the recovery environment. Reviewing storage facilities or inventorying backup media confirms that backups exist and are stored appropriately, but it does not prove they can be restored. Having duplicate equipment available is useful, but it does not confirm that the backup data is readable or usable. The core issue is recoverability, and the only reliable way to validate recoverability is through practical testing. In business continuity and disaster recovery management, testing verifies whether recovery procedures, media, systems, and personnel can achieve required recovery objectives. Therefore, using warm-site equipment to read the backups provides the strongest assurance that backups will be usable when needed.
References:
ISACA CISM Review Manual , Information Security Program Development and Management - backup testing and disaster recovery readiness ISACA CISM Exam Content Outline , Domain 3: Information Security Program Development and Management

NEW QUESTION: 458
Which of the following BEST indicates misalignment of security policies with business objectives?
A. A large number of long-term policy exceptions
B. A large number of user noncompliance incidents
C. Lack of adequate funding for the security program
D. Low completion rate of employee awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 459
Which of the following BEST demonstrates the added value of an information security program?
A. Security baselines
B. A gap analysis

C. A SWOT analysis
D. A balanced scorecard
Answer: (SHOW ANSWER)
A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

NEW QUESTION: 460
An organization wants to migrate a proprietary application to be hosted by a third-party cloud hosting provider using a Platform as a Service (PaaS) model. Prior to selecting the cloud provider, what is MOST important for the organization to ensure?
Freecram.net
A. The cloud provider can meet recovery point objectives (RPOs).
B. The cloud provider adheres to applicable regulations.
C. The cloud provider's service level agreement (SLA) includes availability requirements.
D. The hosting contract has a termination clause.
Answer: (SHOW ANSWER)
When outsourcing to a cloud provider, regulatory compliance is paramount-especially with sensitive or proprietary applications. Non-compliance could result in legal penalties, fines, or reputational damage.
While RPOs, SLAs, and contract clauses are critical components of vendor risk management, ensuring adherence to relevant laws and industry regulations (such as GDPR, HIPAA, PCI DSS) is the first priority in cloud migration decisions.
"Prior to selecting a cloud provider, legal, regulatory, and contractual requirements must be reviewed to ensure alignment."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Considerations in Cloud Computing*

NEW QUESTION: 461
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: 462
Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?
A. To reduce risk mitigation costs
B. To resolve vulnerabilities in enterprise architecture (EA)
C. To manage the risk to an acceptable level
D. To eliminate threats impacting the business
Answer: (SHOW ANSWER)
According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

NEW QUESTION: 463
Which of the following is the PRIMARY outcome of a business impact analysis (BIA)?
A. Streamlining of event triage and implementation of incident response procedures
B. Allocation of budget for technical security controls and enhancements to security culture
C. Assurance of compliance with industry-specific regulations and improvement to business processes
D. Identification of critical business functions and prioritization of recovery efforts
Answer: (SHOW ANSWER)
The primary outcome of a BIA is the identification of critical business functions and prioritization of recovery efforts (D). CISM defines the BIA as the foundation for continuity and resilience planning, providing insight into impact, recovery priorities, and tolerable downtime. The other options represent secondary or unrelated benefits.
References: ISACA CISM Review Manual (Program management-BIA purpose and outcomes); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 464
Which of the following should have the MOST influence on the development of information security policies?
A. Business strategy

B. Past and current threats
C. IT security framework
D. Industry standards
Answer: (SHOW ANSWER)
Business strategy is the overarching driver for any organizational initiative, including security. Information security policies must align with the strategic goals of the organization to ensure relevance, support, and effectiveness.
Security policies that do not consider the business context may hinder operations or fail to protect key objectives. Business-driven policies are more likely to gain executive support and compliance from stakeholders, creating a strong foundation for governance.
"Information security policies must be aligned with business goals and objectives to ensure that they support the overall mission and are embraced by stakeholders."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Strategy Alignment*

NEW QUESTION: 465
Which of the following is the BEST way to obtain organization-wide support for an information security program?
A. Mandate regular security awareness training.
B. Develop security performance metrics.
C. Position security as a business enabler.
D. Prioritize security initiatives based on IT strategy.
Answer: (SHOW ANSWER)
Positioning security as a business enabler is the BEST way to obtain organization-wide support for an information security program, because it helps to demonstrate the value and benefits of security to the organization's strategic objectives, performance, and reputation. By aligning security with the business goals and needs, the information security manager can gain the buy-in and commitment of senior management and other stakeholders, and foster a positive security culture across the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "The information security manager should position information security as a business enabler that supports the achievement of the enterprise's business objectives and adds value to the enterprise." CISM Review Manual, 16th Edition, ISACA, 2020, p. 39: "The information security manager should communicate the value and benefits of information security to senior management and other stakeholders to obtain their support and commitment for the information security program." CISM Review Manual, 16th Edition, ISACA, 2020, p. 40: "The information security manager should promote a positive security culture within the enterprise by influencing the behavior and attitude of employees and other parties toward information security."

NEW QUESTION: 466

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: (SHOW ANSWER)

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

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

NEW QUESTION: 467

When developing an information security strategy for an organization, which of the following is MOST helpful for understanding where to focus efforts?

A. Gap analysis

B. Project plans

C. Vulnerability assessment

D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

Gap analysis is the MOST helpful tool for understanding where to focus efforts when developing an information security strategy for an organization, because it helps to identify the current state and the desired state of the information security governance, and the gaps between them. Gap analysis also helps to prioritize the actions and resources needed to close the gaps and achieve the information security objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Gap analysis is the process of comparing the current state and the desired state of information security governance and identifying the gaps that need to be addressed." CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Gap analysis should be performed periodically to assess the effectiveness and efficiency of the information security strategy and program and to identify the areas for improvement." CISM domain 1: Information security governance [Updated 2022] - Infosec Resources: "Gap analysis: This is a comparison of the current state of security with the desired state. It helps to identify the gaps in security and prioritize the actions required to close them."

NEW QUESTION: 468
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: (SHOW ANSWER)
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: 469

Which of the following would provide the BEST evidence to senior management that security control performance has improved?

A. Demonstrated return on security investment

B. Reduction in inherent risk

C. Results of an emerging threat analysis

D. Review of security metrics trends

Answer: (SHOW ANSWER)

Review of security metrics trends is the best evidence to senior management that security control performance has improved because it helps to measure and demonstrate the effectiveness and efficiency of the security controls over time. Security metrics are quantitative or qualitative indicators that provide information about the security status or performance of an organization, system, process, or activity. Security metrics can be used to evaluate the implementation, operation, and outcome of security controls, such as the number of vulnerabilities detected and remediated, the time to respond and recover from incidents, the compliance level with security policies and standards, or the return on security investment. Review of security metrics trends helps to identify and communicate the progress, achievements, and challenges of the security program, as well as to support decision making and continuous improvement. Therefore, review of security metrics trends is the correct answer.

References:

https://www.bitsight.com/blog/importance-continuous-improvement-security-performance-management

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security- governance-part-2

https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary-cybersecurity- performance-goals.

NEW QUESTION: 470

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

Freecram.net

A. Perform a full data backup.

B. Review the current risk assessment.

C. Update indicators of compromise in the security systems.

D. Conduct ransomware awareness training for all staff.

Answer: (SHOW ANSWER)

NEW QUESTION: 471

An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

A. To facilitate the continuous improvement of the IT organization

B. To ensure controls align with security needs

C. To create and document required IT capabilities

D. To prioritize security risks on a longer scale than the one-year plan

Answer: (SHOW ANSWER)

The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.

The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)

References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3:

Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION: 472

Which of the following is the PRIMARY reason for an information security manager to periodically review existing controls?

A. To prioritize security initiatives

B. To address end-user control complaints

C. To avoid redundant controls

D. To align with emerging risk

Answer: (SHOW ANSWER)

NEW QUESTION: 473

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: 474
Which of the following is MOST important to include in an information security status report management?
A. List of recent security events
B. Key risk indication (KRIs)
C. Review of information security policies
D. information security budget requests
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004

NEW QUESTION: 475
The PRIMARY purpose for conducting cybersecurity risk assessments is to:
A. Assist in security reporting to senior management
B. Provide metrics to indicate cybersecurity program effectiveness
C. Verify compliance across multiple sectors
D. Understand the organization's current security posture
Answer: (SHOW ANSWER)

The main goal of a cybersecurity risk assessment is to gain visibility into the organization's current security posture, identify vulnerabilities, evaluate threats, and understand the potential impact of various risks.
"Risk assessments provide an understanding of the organization's threat landscape, asset vulnerabilities, and residual risk exposure."
- CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Risk Identification* While assessments support reporting and compliance, their primary role is situational awareness.

NEW QUESTION: 476
A global organization is considering its geopolitical security risks. Which of the following is the information security manager's BEST approach?
A. Seek advice from environmental and physical security experts
B. Implement a third-party risk management framework
C. Implement controls that deny access from specific jurisdictions
D. Seek advice from enterprise risk and legal experts
Answer: (SHOW ANSWER)
Geopolitical risk involves complex legal, political, and compliance issues. The enterprise risk and legal teams are best positioned to provide guidance on how national laws, sanctions, and regulations impact operations and security strategies.
"In cases of geopolitical or cross-jurisdictional risk, coordination with legal and enterprise risk functions is essential for informed decision-making."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Context* Security and technical controls should follow this strategic evaluation.

NEW QUESTION: 477
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: (SHOW ANSWER)
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: 478
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: (SHOW ANSWER)
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: 479

An organization ' s main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

A. The information security manager

B. The data owner

C. The application owner

D. The security engineer

Answer: (SHOW ANSWER)

= The application owner is primarily accountable for the associated task because they are responsible for ensuring that the application meets the business requirements and objectives, as well as the security and compliance standards. The application owner is also the one who defines the roles and responsibilities of the application team, including the security engineer, and oversees the development, testing, deployment, and maintenance of the application. The application owner should work with the cloud provider to address the security vulnerability and mitigate the risk. The information security manager, the data owner, and the security engineer are not primarily accountable for the associated task, although they may have some roles and responsibilities in supporting the application owner. The information security manager is responsible for establishing and maintaining the information security program and aligning it with the business objectives and strategy. The data owner is responsible for defining the classification, usage, and protection requirements of the data. The security engineer is responsible for implementing and testing the security controls and features of the application. References = CISM Review Manual 2023, Chapter 1, Section 1.2.2, page 18; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 115.

NEW QUESTION: 480

Which of the following is the BEST way to present the status of an information security program to senior management?

Freecram.net

A. Provide detailed information regarding risk exposure

B. Display concise dashboards

C. Detail the latest security trends

D. Report on root causes of security incidents

Answer: (SHOW ANSWER)

The best way to present the status of an information security program to senior management is to display concise dashboards . CISM governance emphasizes that senior management needs clear, relevant, business- focused information to support decision-making. Dashboards summarize key performance indicators, key risk indicators, control status, incident trends, compliance posture, and risk exposure in a concise and digestible form. Detailed risk information may be useful for risk owners or technical teams, but senior management typically requires summarized insight rather than excessive detail. Security trends and root causes of incidents can provide context, but they do not offer a complete program status view. A well-designed dashboard

enables executives to quickly understand whether the program is effective, aligned with risk appetite, and supporting business objectives. CISM stresses that reporting should be audience-appropriate, actionable, and aligned with governance needs. Therefore, concise dashboards are the best method for presenting information security program status to senior management.
References:
ISACA CISM Review Manual , Information Security Governance - executive reporting and security metrics ISACA CISM Exam Content Outline , Domain 2: Information Security Governance

NEW QUESTION: 481
Which of the following is the MOST important consideration during the design phase of a business impact analysis (BIA)?
A. Selecting quality metrics to monitor business performance
B. Estimating the likelihood that end-to-end processes will be disrupted
C. Obtaining reserve funding to prepare for possible business failures
D. Identifying critical functions for business operations
Answer: (SHOW ANSWER)
The design phase of a BIA must begin with identifying critical business functions, since they determine:
Which systems/processes need protection
Recovery priorities
Acceptable downtime (RTO/MTD)
Without clearly defining what ' s critical, the BIA cannot guide resource allocation or continuity strategies effectively.
"A successful BIA must begin with identifying which business functions are critical to achieving organizational objectives."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery, Section: BIA Methodology*

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

NEW QUESTION: 482

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

A. Revise the procurement process.

B. Update the change management process.

C. Discuss the issue with senior leadership.

D. Remove the application from production.

Answer: (SHOW ANSWER)

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

The information security manager should explain the potential impact and consequences of the incident, and recommend corrective actions to remediate the situation. The information security manager should also review the root cause of the incident and identify any gaps or weaknesses in the existing policies, procedures, or controls that allowed the business unit to implement the new application without proper authorization, testing, or documentation. The information security manager should then revise the procurement process, update the change management process, or implement other measures to prevent similar incidents from occurring in the future. Removing the application from production may not be feasible or desirable, depending on the business needs and the severity of the risks involved. References = CISM Review Manual,
16th Edition, pages 100-1011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page
2692

Learn more:

1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 483

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: (SHOW ANSWER)

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: 484

Which of the following BEST ensures information security governance is aligned with corporate governance?

A. A security steering committee including IT representation

B. A consistent risk management approach

C. An information security risk register

D. Integration of security reporting into corporate reporting

Answer: (SHOW ANSWER)

The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with corporate governance by themselves. References = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

NEW QUESTION: 485

Which of the following should be done FIRST to prioritize response to incidents?

A. Escalation

B. Analysis

C. Containment

D. Triage

Answer: C (LEAVE A REPLY)

NEW QUESTION: 486

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

A. Modifying its predefined configuration automatically based on malicious traffic

B. Restricting external traffic within a private network

C. Redirecting distributed denial-of-service attacks

D. Filtering incoming Hypertext Transfer Protocol traffic

Answer: (SHOW ANSWER)

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

Redirecting distributed denial-of-service attacks is usually handled by DDoS protection services, content delivery networks, or traffic scrubbing solutions. In CISM terms, the correct control must match the risk and technology layer being protected. Since a WAF protects web applications by filtering web traffic, option D is the best answer.
Reference: CISM Information Security Program Development and Management; technical security controls, application protection, and web application security principles.

NEW QUESTION: 487
Which of the following is MOST helpful in the development of a cost-effective information security strategy that is aligned with business requirements?
A. Developing policy standards
B. Benchmarking against industry peers
C. Categorizing information assets
D. Enforcing data retention
Answer: B (LEAVE A REPLY)

NEW QUESTION: 488
An organization implemented a number of technical and administrative controls to mitigate risk associated with ransomware. Which of the following is MOST important to present to senior management when reporting on the performance of this initiative?
A. The total cost of the investment
B. The cost and associated risk reduction
C. The number and severity of ransomware incidents
D. Benchmarks of industry peers impacted by ransomware
Answer: (SHOW ANSWER)
The most important information to present to senior management when reporting on the performance of the initiative to mitigate risk associated with ransomware is the cost and associated risk reduction, which means showing the value and effectiveness of the technical and administrative controls in terms of reducing the likelihood and impact of ransomware incidents and data extortion, and comparing them with the investment and resources required to implement and maintain them. The cost and associated risk reduction can help senior management to evaluate the return on investment (ROI) and the alignment with the business objectives and risk appetite of the initiative.
References = Ransomware Risk Management - NIST, #StopRansomware Guide | CISA

NEW QUESTION: 489
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?
A. Training project managers on risk assessment
B. Integrating the risk assessment into the internal audit program
C. Applying global security standards to the IT projects

D. Having the information security manager participate on the project steering committees
Answer: D (LEAVE A REPLY)

NEW QUESTION: 490
Which of the following is the MOST important criterion when deciding whether to accept residual risk?
A. Cost of replacing the asset
B. Cost of additional mitigation
C. Annual loss expectancy (ALE)
D. Annual rate of occurrence
Answer: (SHOW ANSWER)
= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one-year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk event occurring within a one-year period, and SLE is the estimated cost of a single occurrence of a risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance. Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
22, page 242

NEW QUESTION: 491
Which of the following is an information security manager's BEST recommendation to senior management following a breach at the organization's Software as a Service (SaaS) vendor?
A. Engage legal counsel.
B. Renegotiate the vendor contract.
C. Terminate the relationship with the vendor.
D. Update the vendor risk assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 492
As part of a risk assessment, a security control was discovered to be inadequate. When assigning a risk owner, which of the following attributes is MOST important to consider?
A. The risk owner is able to reassess the risk following remediation.
B. The risk owner has the authority to take action on the risk.
C. The risk owner is able to make timely updates to the risk register.
D. The risk owner also owns the associated control that failed.

Answer: (SHOW ANSWER)
The most important attribute when assigning a risk owner is that the risk owner has the authority to take action on the risk (B). In CISM, risk ownership is fundamentally about accountability and decision-making authority. The risk owner must be empowered to decide on risk treatment options-such as mitigation, transfer, acceptance, or avoidance-and to allocate resources or approve changes necessary to address the risk.
While reassessing risk after remediation (A) and updating the risk register (C) are important responsibilities, they are administrative and follow-on activities that do not, by themselves, ensure effective risk management.
Ownership of the failed control (D) is not required; in fact, CISM distinguishes between risk ownership (business accountability) and control ownership (operational responsibility). The risk owner is typically a business role accountable for the impact of the risk, not necessarily the individual responsible for implementing or operating the control.
CISM guidance consistently stresses that risk owners must have sufficient authority, accountability, and understanding of business impact to make informed decisions aligned with the organization's risk appetite.
Without authority, risk ownership becomes ineffective and purely symbolic.
References:
ISACA CISM Review Manual, Information Risk Management - risk ownership, accountability, and risk response ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

NEW QUESTION: 493
Which of the following is an example of risk mitigation?
A. Purchasing insurance
B. Discontinuing the activity associated with the risk
C. Improving security controls
D. Performing a cost-benefit analysis
Answer: (SHOW ANSWER)
Improving security controls is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. Risk mitigation can be achieved by implementing various strategies, such as purchasing insurance, discontinuing the activity associated with the risk, or improving security controls. Purchasing insurance is a form of risk transfer, which is the process of shifting the responsibility or burden of a risk to another party. Discontinuing the activity associated with the risk is a form of risk avoidance, which is the process of eliminating or avoiding a potential source of harm. Performing a cost-benefit analysis is a form of risk evaluation, which is the process of assessing the costs and benefits of different options to manage a risk. References = CISM Review Manual, 16th Edition, page 1741; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 802

NEW QUESTION: 494
A recovery point objective (RPO) is required in which of the following?

A. Disaster recovery plan (DRP)
B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)
A recovery point objective (RPO) is required in a disaster recovery plan (DRP), because it indicates the earliest point in time to which it is acceptable to recover data after a disaster. It effectively quantifies the permissible amount of data loss in case of interruption. It is determined based on the acceptable data loss in case of disruption of operations1. A DRP is a document that defines the procedures, resources, and actions to restore the critical IT systems and data in the event of a disaster that affects the normal operations of the organization2. A DRP should include the RPO for each critical system and data, as well as the backup and restoration methods, frequency, and location to achieve the RPO3.
A RPO is not required in an information security plan, an incident response plan, or a business continuity plan (BCP), because these plans have different purposes and scopes. An information security plan is a document that defines the objectives, policies, standards, and guidelines for information security management in the organization4. An incident response plan is a document that defines the procedures, roles, and responsibilities for identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. A BCP is a document that defines the procedures, resources, and actions to ensure the continuity of the essential business functions and processes in the event of a disruption that affects the normal operations of the organization. These plans may include other metrics, such as recovery time objective (RTO), which is the amount of time after a disaster in which business operation is resumed, or resources are again available for use, but they do not require a RPO.
References = 1: IS Disaster Recovery Objectives - RunModule 2: Information System Contingency Planning Guidance - ISACA 3: CISM Certified Information Security Manager - Question1411 4: CISM Review Manual, 16th Edition, ISACA, 2021, page 23. : CISM Review Manual, 16th Edition, ISACA, 2021, page 223.
CISM Review Manual, 16th Edition, ISACA, 2021, page 199. : RTO vs. RPO - What is the difference? - Advisera

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