ISACA.CISM.v2026-05-07.q517

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	517
Version:	v2026-05-07
# of views:	103
# of Questions views:	5529
https://www.freecram.net/torrent/ISACA.CISM.v2026-05-07.q517.html	

NEW QUESTION: 1
Which of the following BEST enables the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption?
A. Service level agreement (SLA)
B. Business continuity plan (BCP)
C. Disaster recovery plan (DRP)
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
The best option to enable the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption is B. Business continuity plan (BCP). This is because a BCP is a documented collection of procedures and information that guides the organization to prepare for, respond to, and recover from a disruption, such as a natural disaster, a cyberattack, or a pandemic. A BCP aims to ensure the continuity of the critical business functions and processes that support the delivery of products and services to the customers and stakeholders. A BCP also defines the roles, responsibilities, resources, and actions required to maintain the operational resilience of the organization in the face of a disruption.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.3, page 2141; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 6, page 3

NEW QUESTION: 2
Which of the following should an information security manager do FIRST when a vulnerability has been disclosed?
A. Perform a patch update.
B. Conduct a risk assessment.
C. Perform a penetration test.

D. Conduct an impact assessment.

Answer: (SHOW ANSWER)

According to the CISM Review Manual, the first step an information security manager should take when a vulnerability has been disclosed is to conduct a risk assessment to determine the likelihood and impact of the vulnerability being exploited, and the appropriate response strategy. Performing a patch update, a penetration test or an impact assessment are possible subsequent steps, but not the first one.

References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.3.2, page 1331.

NEW QUESTION: 3

Which of the following should be done FIRST when developing a business continuity plan (BCP)?

A. Review current recovery policies.

B. Prioritize the critical processes.

C. Define the organizational strategy.

D. Review existing cyber insurance coverage.

Answer: (SHOW ANSWER)

NEW QUESTION: 4

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

NEW QUESTION: 5

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: A (LEAVE A REPLY)
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: 6
Which of the following is the FIRST step in developing a business continuity plan (BCP)?
A. Identify the applications with the shortest recovery time objectives (RTOs).
B. Determine the business recovery strategy.
C. Determine available resources.
D. Identify critical business processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
The PRIMARY goal when conducting post-incident reviews is to identify:
A. Additional cybersecurity budget needs
B. Weaknesses in incident response plans
C. Information to be shared with senior management
D. Individuals that need additional training
Answer: (SHOW ANSWER)
The core objective of a post-incident review (PIR) is to identify gaps and weaknesses in the response process.
This includes missteps, delays, communication failures, or policy limitations - all of which provide insight to improve future incident handling.
"Post-incident reviews focus on identifying root causes and areas for improvement to enhance the organization's preparedness for future incidents."

- CISM Review Manual 15th Edition, Chapter 4: Post-Incident Activities* Though training, reporting, and budgeting may follow, they are secondary outcomes of this process.

NEW QUESTION: 8
Which of the following is the BEST indication that an organization has a mature information security culture?
A. Information security training is mandatory for all staff.
B. The organization's information security policy is documented and communicated.
C. The chief information security officer (CISO) regularly interacts with the board.
D. Staff consistently consider risk in making decisions.
Answer: (SHOW ANSWER)
The BEST indication that an organization has a mature information security culture is when its staff consistently consider risk in making decisions. When an organization's staff understands the risks associated with their actions and are empowered to make risk-informed decisions, it indicates that the organization has a mature information security culture.
According to the Certified Information Security Manager (CISM) Study Manual, "A mature information security culture exists when the people within the organization understand and appreciate the risks associated with information and technology and when they take steps to manage those risks on a daily basis." While information security training, documented information security policies, and regular interaction between the chief information security officer (CISO) and the board are all important components of a mature information security culture, they are not sufficient on their own. It is only when staff consistently consider risk in making decisions that an organization's information security culture can be considered mature.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 151-152.

NEW QUESTION: 9
Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software. What is the BEST way for the information security manager to help senior management understand the related risk?
A. Include the impact of the risk as part of regular metrics.
B. Recommend the security steering committee conduct a review.
C. Update the risk assessment at regular intervals
D. Send regular notifications directly to senior managers
Answer: (SHOW ANSWER)
Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its

impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact.
References: https://www.isaca.
org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security-investments
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of- your-information-security-management-system

NEW QUESTION: 10

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: 11
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?
A. The benefit is greater than the potential risk.
B. USB storage devices are enabled based on user roles.

C. Users accept the risk of noncompliance.
D. Access is restricted to read-only.
Answer: (SHOW ANSWER)
The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security pol-icy should also be aligned with the organization's business objectives and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2. The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as:
*Enhancing data mobility and accessibility
*Improving data backup and recovery
*Supporting data sharing and collaboration
*Enabling data encryption and authentication
However, USB storage devices also pose significant security risks for users and organi-zations, such as:
*Introducing malware or viruses to laptops and desktops
*Exposing sensitive data to unauthorized access or disclosure
*Losing or stealing data due to device loss or theft
*Violating security policies or regulations
Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of

users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4.
Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5.
References: 1:
Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

NEW QUESTION: 12
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: 13
Which of the following should be the PRIMARY consideration when developing an incident response plan?
A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents
Answer: (SHOW ANSWER)
Management support is the primary consideration when developing an incident response plan, as it is essential for obtaining the necessary resources, authority, and commitment for the plan. Management support also helps to ensure that the plan is aligned with the organization's

business objectives, risk appetite, and security strategy, and that it is communicated and enforced across the organization. Management support also facilitates the coordination and collaboration among different stakeholders, such as business units, IT functions, legal, public relations, and external parties, during an incident response.
The definition of an incident (A) is an important component of the incident response plan, as it provides the criteria and thresholds for identifying, classifying, and reporting security incidents. However, the definition of an incident is not the primary consideration, as it is derived from the organization's security policies, standards, and procedures, and may vary depending on the context and impact of the incident.
Compliance with regulations (B) is also an important factor for the incident response plan, as it helps to ensure that the organization meets its legal and contractual obligations, such as notifying the authorities, customers, or partners of a security breach, preserving the evidence, and reporting the incident outcomes.
However, compliance with regulations is not the primary consideration, as it is influenced by the nature and scope of the incident, and the applicable laws and regulations in different jurisdictions.
Previously reported incidents (D) are a valuable source of information and lessons learned for the incident response plan, as they help to identify the common types, causes, and impacts of security incidents, as well as the strengths and weaknesses of the current incident response processes and capabilities. However, previously reported incidents are not the primary consideration, as they are not predictive or comprehensive of the future incidents, and may not reflect the changing threat landscape and business environment.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 181-1821 Learn more:

NEW QUESTION: 14
Management has expressed concerns to the information security manager that shadow IT may be a risk to the organization. What is the FIRST step the information security manager should take?
A. Determine the extent of shadow IT usage
B. Update the security policy to address shadow IT
C. Block the end user's ability to use shadow IT
D. Determine the value of shadow IT projects
Answer: (SHOW ANSWER)
The first step is to determine the extent of shadow IT usage (A). CISM emphasizes understanding the current state before implementing controls or policy changes. Without knowing where and how shadow IT exists, actions such as blocking usage (C) or updating policy (B) may disrupt business operations unnecessarily.
Evaluating value (D) is secondary. Identifying scope enables informed risk assessment and proportionate response.
References: ISACA CISM Review Manual (Governance-risk identification and assessment); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 15
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: 16
An employee who is a remote user has copied financial data from the corporate server to a laptop using virtual private network (VPN) connectivity. Which of the following is the MOST important factor to determine if it should be classified as a data leakage incident?
A. Valid use case
B. Employee's job role
C. Ownership of the data
D. Review of the audit logs
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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 17
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: (SHOW ANSWER)
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: 18
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: 19
Which of the following is the BEST indicator of the maturity level of a vendor risk management process?
A. Average time required to complete the vendor risk management process
B. Percentage of vendors that have gone through the vendor onboarding process
C. Percentage of vendors that are regularly reviewed against defined criteria
D. Number of vendors rejected because of security review results
Answer: (SHOW ANSWER)
The percentage of vendors that are regularly reviewed against defined criteria is the best indicator of the maturity level of a vendor risk management process, as it reflects the extent to which the organization has established and implemented a consistent, repeatable, and effective process to monitor and evaluate the security performance and compliance of its vendors. A high percentage indicates a mature process that covers all vendors and applies clear and relevant criteria based on the organization's risk appetite and objectives. A low percentage indicates a less mature process that may be ad hoc, incomplete, or outdated. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 20
A. A validation of the current firewall rule set
B. A port scan of the firewall from an internal source
C. A ping test from an external source
D. A simulated denial of service (DoS) attack against the firewall
Answer: (SHOW ANSWER)
A validation of the current firewall rule set is the best method for determining whether a firewall has been configured to provide a comprehensive perimeter defense because it verifies that the firewall rules are consistent, accurate, and effective in allowing or blocking traffic according to the security policies and standards of the organization. A port scan of the firewall from an internal source is not a good method because it does not test the firewall's behavior from an external perspective, which is more relevant for perimeter defense. A ping test from an external source is not a good method because it only tests the firewall's availability and responsiveness, not its security or functionality. A simulated denial of service (DoS) attack against the firewall is not a good method because it only tests the firewall's resilience and performance under high traffic load, not its security or functionality. 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/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca- journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 21
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: 22
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: 23
Which of the following is necessary to ensure consistent protection for an organization's information assets?
A. Classification model
B. Control assessment
C. Data ownership
D. Regulatory requirements
Answer: (SHOW ANSWER)
The answer to the question is A. Classification model. This is because a classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by:
Providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets Enabling the identification and prioritization of the information assets that need the most protection and resources Facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification Supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) A classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets, enabling the identification and prioritization of the information assets that need the most protection and resources, facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification, and supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISA Domain 5 - Protection of Information Assets2; CISM domain 3: Information security program development and management [2022 update]3; CISM Domain 2: Information Risk Management (IRM) [2022 update]4

NEW QUESTION: 24

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: 25

An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. notify the business process owner.

B. follow the business continuity plan (BCP).

C. conduct an incident forensic analysis.

D. follow the incident response plan.

Answer: (SHOW ANSWER)

= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =

1: CISM Review Manual 15th Edition, page 199-2004

2: CISM Practice Quiz, question 1011

3: Computer Security Incident Handling Guide5, page 2-3

NEW QUESTION: 26

Which of the following is the BEST option to lower the cost to implement application security controls?

A. Perform security tests in the development environment.

B. Integrate security activities within the development process

C. Perform a risk analysis after project completion.

D. Include standard application security requirements

Answer: (SHOW ANSWER)

Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios. Performing a risk analysis after project completion is not a good option because it may be too late to identify or mitigate security risks that may have been introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software- development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems

NEW QUESTION: 27

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

A. Establish key risk indicators (KRIs).

B. Use quantitative risk assessment methods.

C. Provide regular reporting on risk treatment to senior management

D. Require steering committee approval of risk treatment plans.

Answer: (SHOW ANSWER)

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

the status and results of the risk treatment process and to obtain feedback and support from senior management.
However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter
2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION: 28
A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems. The vendor has released an emergency patch. Which of the following should be the information security managers PRIMARY concern?
A. Documentation of patching procedures
B. Ability to test the patch prior to deployment
C. Availability of resources to implement controls
D. Adequacy of the incident response plan
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following is the MOST effective way to detect security incidents?
A. Analyze recent security risk assessments.
B. Analyze security anomalies.
C. Analyze penetration test results.
D. Analyze vulnerability assessments.
Answer: (SHOW ANSWER)
Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

NEW QUESTION: 30
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: 31
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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 32
In a business proposal, a potential vendor promotes being certified for international security standards as a measure of its security capability.
Before relying on this certification, it is MOST important that the information security manager confirms that the:
A. current international standard was used to assess security processes.
B. certification will remain current through the life of the contract.
C. certification scope is relevant to the service being offered.
D. certification can be extended to cover the client's business.
Answer: (SHOW ANSWER)
Before relying on a vendor's certification for international security standards, such as ISO/IEC 27001, it is most important that the information security manager confirms that the certification scope is relevant to the service being offered. The certification scope defines the boundaries and applicability of the information security management system (ISMS) that the vendor has implemented and audited. The scope should cover the processes, activities, assets, and locations that are involved in delivering the service to the client. If the scope is too narrow, too broad, or not aligned with the service, the certification may not provide sufficient assurance of the vendor's security capability and performance.
The current international standard was used to assess security processes (A) is an important factor, but not the most important one. The information security manager should verify that the vendor's certification is based on the latest version of the standard, which reflects the current best practices and requirements for information security. However, the standard itself is generic and adaptable, and does not prescribe specific security controls or solutions. Therefore, the certification does not guarantee that the vendor has implemented the most appropriate or effective security processes for the service being offered.
The certification will remain current through the life of the contract (B) is also an important factor, but not the most important one. The information security manager should ensure that the vendor's certification is valid and up to date, and that the vendor maintains its compliance with the standard throughout the contract period.
However, the certification is not a one-time event, but a continuous process that requires periodic surveillance audits and recertification every three years. Therefore, the certification does not ensure that the vendor's security capability and performance will remain consistent or satisfactory for the duration of the contract.
The certification can be extended to cover the client's business (D) is not a relevant factor, as the certification is specific to the vendor's ISMS and does not apply to the client's business. The information security manager should not rely on the vendor's certification to substitute or supplement the client's own security policies, standards, or controls. The information security

manager should conduct a due diligence and risk assessment of the vendor, and establish a clear and comprehensive service level agreement (SLA) that defines the security roles, responsibilities, expectations, and metrics for both parties.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, page 142-1431

NEW QUESTION: 33
The effectiveness of an incident response team will be GREATEST when:
A. incidents are identified using a security information and event monitoring (SIEM) system.
B. the incident response process is updated based on lessons learned,
C. the incident response team members are trained security personnel,
D. the incident response team meets on a regular basis to review log files
Answer: (SHOW ANSWER)

NEW QUESTION: 34
The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:
A. the organization has the required funds to implement the plan.
B. compliance with legal and regulatory requirements.
C. staff participation in information security efforts.
D. the plan aligns with corporate governance.
Answer: (SHOW ANSWER)
The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly1. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization2. The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives3. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation4. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253:
CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA,
2017, page 27.
Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It

is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION: 35
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. Provide awareness training to the CEO for this type of phishing attack.
B. Provide awareness training to staff responsible for wire transfers.
C. Temporarily suspend wire transfers for the organization.
D. Disable emails for staff responsible for wire transfers.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following is MOST effective in gaining support for the information security strategy from senior management?
A. Business impact analysis (BIA) results
B. A major breach at a competitor
C. Third-party security audit results
D. Cost-benefit analysis results
Answer: (SHOW ANSWER)
Senior management engagement is most effectively achieved when information security risks are clearly connected to real, tangible business consequences. A major breach at a competitor (B) provides a credible, industry-relevant example that demonstrates potential financial, operational, reputational, and regulatory impacts in a way executives readily understand. While BIA results (A), audit findings (C), and cost-benefit analyses (D) are important inputs, they are often abstract or internally focused. CISM guidance emphasizes that executive support is strongest when security messaging is business-driven, externally validated, and tied to strategic risk awareness. A peer breach highlights that the threat is realistic, imminent, and applicable to the organization's context, which increases urgency and executive buy-in for the security strategy.
References: ISACA CISM Review Manual (Governance-executive communication, stakeholder engagement); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 37
Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?
A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions
C. Effective protection of information assets
D. Optimized allocation of recovery resources
Answer: (SHOW ANSWER)

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

NEW QUESTION: 38
Which of the following is MOST important to determine following the discovery and eradication of a malware attack?
A. The type of malware involved
B. The malware entry path
C. The method of detecting the malware
D. The creator of the malware
Answer: (SHOW ANSWER)

NEW QUESTION: 39
An organization engages a third-party vendor to monitor and support a financial application under scrutiny by regulators. Which of the following controls would MOST effectively manage risk to the organization?
A. Monitoring key risk indicators (KRIs)
B. Implementing separation of duties between systems and data
C. Disabling vendor access and only re-enabling when access is needed
D. Including penalty clauses for noncompliance in the vendor contract
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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: 41
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: 42
The MOST important reason for having an information security manager serve on the change management committee is to:
A. identify changes to the information security policy.
B. ensure that changes are tested.
C. ensure changes are properly documented.
D. advise on change-related risk.
Answer: (SHOW ANSWER)
The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2.
The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the

information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.

The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes.

Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk.

Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk.

References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION: 43

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

A. Standards

B. Procedures

C. Regulations

D. Baselines

Answer: (SHOW ANSWER)

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

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

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

References:

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

NEW QUESTION: 44

When properly implemented, secure transmission protocols protect transactions:

A. from eavesdropping.

B. from denial of service (DoS) attacks.

C. on the client desktop.

D. in the server's database.

Answer: (SHOW ANSWER)

Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information1. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party. Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage2. Therefore, secure

transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures3. Some examples of secure transmission protocols are:

* Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.
* Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.
* Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port forwarding, which allows secure tunneling of other network services through SSH connections.

References = 1: 6 Network Security Protocols You Should Know | Cato Networks 2: Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL /TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec - Wikipedia : Secure Shell - Wikipedia

NEW QUESTION: 45

Which of the following is the BEST way to contain an SQL injection attack that has been detected by a web application firewall?

A. Force password changes on the SQL database.
B. Reconfigure the web application firewall to block the attack.
C. Update the detection patterns on the web application firewall.
D. Block the IPs from where the attack originates.

Answer: (SHOW ANSWER)

According to the CISM Review Manual, one of the best ways to contain an SQL injection attack that has been detected by a web application firewall is to reconfigure the web application firewall to block the attack.
This means that the web application firewall should be updated with the latest detection patterns and rules that can identify and prevent SQL injection attacks. By doing so, the web application firewall can reduce the impact and damage of the attack, and prevent further exploitation of the vulnerable database1 The other options are not as effective as reconfiguring the web application firewall to block the attack. Force password changes on the SQL database is a reactive measure that does not address the root cause of the problem, and may cause data loss or corruption if not done properly. Updating the detection patterns on the web application firewall is a preventive measure that can help to detect SQL injection attacks, but it does not stop them from happening in the first place. Blocking IPs from where the attack originates is a defensive measure that can limit or stop some SQL injection attacks, but it does not protect all possible sources of malicious traffic, and may also affect legitimate users or applications1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 32-33...

NEW QUESTION: 46
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".

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 47

Which of the following is MOST important to have in place when conducting a security control assessment of a system?

A. Security documentation

B. Assurance test plan

C. Scanning tools

D. Control specifications

Answer: (SHOW ANSWER)

NEW QUESTION: 48

Conducting log analysis falls into which phase of the incident management life cycle?

A. Post-incident

B. Containment

C. Detection

D. Planning

Answer: (SHOW ANSWER)

Log analysis is a core detection activity (C) within the incident management lifecycle. Logs provide evidence of abnormal activity, policy violations, or indicators of compromise that enable security teams to identify potential incidents. While logs may also be reviewed during post-incident analysis, their primary role in the lifecycle is to detect events and trigger incident response. Containment (B) focuses on limiting damage after an incident is confirmed, and planning (D) involves preparation activities such as procedures and roles. CISM emphasizes strong detection capabilities-including log monitoring, SIEM, and alerting-as essential to reducing mean time to detect (MTTD) and limiting business impact.

References: ISACA CISM Review Manual (Incident management-lifecycle phases, detection and monitoring); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 49

Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy

B. Risk management framework

C. Risk appetite

D. Security standards

Answer: (SHOW ANSWER)

= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are

effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION: 50

An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

Preetram.net

A. Internal IT audit
B. The data custodian
C. The information security manager
D. The data owner
Answer: (SHOW ANSWER)
The data owner is the person who has the authority and responsibility to classify, grant access, and monitor the use of the CRM data. The data owner should ensure that the data is protected according to its classification and business requirements. The data custodian is the person who implements the controls and procedures to protect the data as directed by the data owner. The information security manager is the person who advises the data owner on the best practices and standards for data security. The internal IT audit is the function that evaluates the effectiveness and compliance of the data security controls and procedures.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Roles and Responsibilities, Subsection: Data Owner, Page 23.

NEW QUESTION: 51
Which of the following business units should own the data that populates an identity management system?
A. Information security
B. Legal
C. Information technology
D. Human resources (HR)
Answer: (SHOW ANSWER)

NEW QUESTION: 52
A small organization with limited budget hires a new information security manager who finds the same IT staff member is assigned the responsibility of system administrator, security administrator, database administrator (DBA), and application administrator What is the manager's BEST course of action?
A. Formally document IT administrator activities.
B. Automate user provisioning activities.
C. Maintain strict control over user provisioning activities.
D. Implement monitoring of IT administrator activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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: 54
Implementing the principle of least privilege PRIMARILY requires the identification of:
A. job duties
B. data owners
C. primary risk factors.
D. authentication controls
Answer: (SHOW ANSWER)
Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources. The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.
The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users.
Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege,

but they are not the ones who determine the job duties of the users. References = Principle of least privilege What Is the Principle of Least Privilege and Why is it Important? - F5 1
4

NEW QUESTION: 55
Which of the following BEST supports investments in an information security program?
A. Business cases
B. Business impact analysis (BIA)
C. Risk assessment results
D. Gap analysis results
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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.

NEW QUESTION: 57
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: D (LEAVE A REPLY)
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: 58
Which type of plan is PRIMARILY intended to reduce the potential impact of security events that may occur?
A. Disaster recovery plan (DRP)
B. Security awareness plan
C. Incident response plan
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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. Engaging an external audit
B. Enforcing strong monitoring controls
C. Establishing compensating controls
D. Conducting a gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Of the following, who is BEST positioned to be accountable for risk acceptance decisions based on risk appetite?
Freecram.net
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: 61

Following an unsuccessful denial of service (DoS) attack, identified weaknesses should be:
A. quickly resolved and eliminated regardless of cost.
B. noted and re-examined later if similar weaknesses are found.
C. tracked and reported on until their final resolution.
D. documented in security awareness programs.
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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 62
Which of the following would be MOST important to include in communications to customers impacted by an information security incident?
A. Details of the type of data exposed
B. Identities of the attackers
C. Costs of the incident to the organization
D. Technical information related to the incident
Answer: (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: 63
Which risk is introduced when using only sanitized data for the testing of applications?
A. Data loss may occur during the testing phase.
B. Data disclosure may occur during the migration event
C. Unexpected outcomes may arise in production
D. Breaches of compliance obligations will occur.
Answer: (SHOW ANSWER)
Unexpected outcomes may arise in production when using only sanitized data for the testing of applications.
Sanitized data is data that has been purposely and permanently deleted or modified to prevent unauthorized access or misuse. Sanitized data may not reflect the real characteristics, patterns, or behaviors of the original data, and thus may not be suitable for testing applications that rely on data quality and accuracy. According to NIST, data sanitization methods can affect the usability of data for testing purposes1. The other options are not risks introduced by using sanitized data for testing applications, but rather risks that can be mitigated by using sanitized data. Data loss, data disclosure, and breaches of compliance obligations are possible consequences of using unsanitized data that contains sensitive or confidential information. References: 2:
What is Data Sanitization? | Data Erasure Methods | Imperva 3: Data sanitization techniques: Standards, practices, legislation 1: Data sanitization - Wikipedia

NEW QUESTION: 64
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: 65

Which of the following MUST happen immediately following the identification of a malware incident?

A. Preparation

B. Recovery

C. Containment

D. Eradication

Answer: (SHOW ANSWER)

Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident12. Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently12. Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure12. Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware incident12. References = 1: CISM Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA2

NEW QUESTION: 66

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: 67
Which of the following components of an information security risk assessment is MOST valuable to senior management?
A. Threat profile
B. Residual risk
C. Return on investment (ROI)
D. Mitigation actions
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after implementing risk mitigation actions. It is the most valuable component for senior management because it helps them to evaluate the effectiveness and efficiency of risk management and make informed decisions about risk acceptance, transfer or avoidance. References = CISM Review Manual, 16th Edition, Chapter 2, Section 2.3.41

NEW QUESTION: 68
The PRIMARY benefit of integrating information security activities into change management processes is to:
A. protect the organization from unauthorized changes.
B. protect the business from collusion and compliance threats.
C. ensure required controls are included in changes.
D. provide greater accountability for security-related changes in the business.
Answer: (SHOW ANSWER)

NEW QUESTION: 69

Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. a function of the likelihood and impact, should a threat exploit a vulnerability.

B. the magnitude of the impact, should a threat exploit a vulnerability.

C. a function of the cost and effectiveness of controls over a vulnerability.

D. the likelihood of a given threat attempting to exploit a vulnerability

Answer: (SHOW ANSWER)

= According to the CISM Manual1, risk is defined as the combination of the probability of an event and its consequence. Therefore, determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as a function of the likelihood and impact, should a threat exploit a vulnerability.

Likelihood is the probability or frequency of a threat occurring, while impact is the magnitude or severity of the harm or loss that would result from a threat exploiting a vulnerability. The higher the likelihood and impact, the higher the risk. The lower the likelihood and impact, the lower the risk.

The other options are not correct because they do not capture the full expression of risk. Option B only considers the impact, but not the likelihood, of a threat exploiting a vulnerability. Option C confuses the risk with the risk response, which is the action taken to reduce or mitigate the risk. Option D only considers the likelihood, but not the impact, of a threat attempting to exploit a vulnerability.

References = CISM Manual1, Chapter 2: Information Risk Management (IRM), Section 2.1: Risk Concepts2

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

NEW QUESTION: 70

Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?

Freecram.net

A. Risk assessment

B. Business impact analysis (BIA)

C. Penetration test results

D. Vulnerability scan results

Answer: (SHOW ANSWER)

Risk assessment is the BEST input to a business case for a technical solution to address potential system vulnerabilities, because it helps to identify and prioritize the most critical risks that the solution should mitigate or reduce. Risk assessment also helps to evaluate the costs and benefits of the solution in terms of reducing the likelihood and impact of potential threats and incidents.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 47: "Risk assessment is the process of identifying and analyzing information security risks and determining their potential impact on the enterprise's business objectives." CISM Review Manual, 16th Edition, ISACA, 2020, p. 48: "Risk

assessment provides input to the business case for information security investments by identifying and prioritizing the most critical risks that need to be addressed and evaluating the costs and benefits of the proposed solutions."

NEW QUESTION: 71
Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?
A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan
Answer: (SHOW ANSWER)
The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type, scope, and complexity of the forensic investigation, the legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The existence of the provider's incident response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any

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

NEW QUESTION: 72
Predetermined containment methods to be used in a cybersecurity incident response should be based PRIMARILY on the:
A. number of impacted users.
B. capability of incident handlers.
C. type of confirmed incident.
D. predicted incident duration.
Answer: (SHOW ANSWER)
According to the NIST SP 800-61 Computer Security Incident Handling Guide, the type of confirmed incident is one of the most important criteria for choosing a containment strategy, as different types of incidents may require different levels of urgency, scope, and impact1. For example, a denial-of-service attack may require a different containment strategy than a ransomware attack or a data breach.
References = 1: NIST SP 800-61: 3.1. Choosing a Containment Strategy2

NEW QUESTION: 73
Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?
A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents
Answer: (SHOW ANSWER)
Increasing accountability is the primary reason for ensuring clearly defined roles and responsibilities are communicated to users who have been granted administrative privileges due to specific application requirements. Administrative privileges grant users the ability to perform actions that can affect the security, availability and integrity of the application or system, such as installing software, modifying configurations, accessing sensitive data or granting access to other users. Therefore, users who have administrative privileges must be aware of their roles and responsibilities and the consequences of their actions. Communicating clearly defined roles and responsibilities to these users helps to establish accountability by setting expectations, defining boundaries, assigning ownership and enabling monitoring and reporting. Accountability also helps

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

NEW QUESTION: 74
An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?
A. Control owner responses based on a root cause analysis
B. The impact of noncompliance on the organization's risk profile
C. A noncompliance report to initiate remediation activities
D. A business case for transferring the risk
Answer: (SHOW ANSWER)
The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps

them understand the potential consequences of not adhering to the established controls and the need for corrective actions.
Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process." CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

NEW QUESTION: 75
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. hand over the controls to the relevant business owners.
B. ensure the controls are regularly tested for ongoing effectiveness.
C. perform testing to compare control performance against industry levels.
D. prepare to adapt the controls for future system upgrades.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An organization is considering using a third party to host sensitive archived data. Which of the following is MOST important to verify before entering into the relationship?
A. The vendor's data centers are in the same geographic region.
B. The encryption keys are not provisled to the vendor.
C. The vendor's controls are in line with the organization's security standards.
D. Independent audits of the vendor's operations are regularly conducted.
Answer: (SHOW ANSWER)
The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor's controls are in line with the organization's security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 77
Which of the following is the MOST important objective when planning an incident response program?
A. Managing resources
B. Recovering from a disaster
C. Ensuring IT resiliency
D. Minimizing business impact
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following will ensure confidentiality of content when accessing an email system over the Internet?
A. Multi-factor authentication
B. Digital encryption
C. Data masking
D. Digital signatures
Answer: (SHOW ANSWER)
Digital encryption is the process of transforming data into an unreadable form using a secret key or algorithm.
Digital encryption will ensure the confidentiality of content when accessing an email system over the Internet, as it prevents unauthorized parties from intercepting, viewing, or modifying the email messages. Digital encryption can be applied to both the email content and the email transmission, using different methods such as symmetric encryption, asymmetric encryption, or hybrid encryption. Digital encryption can also provide other benefits such as authentication, integrity, and non-repudiation, depending on the encryption scheme and the use of digital signatures or certificates. References = CISM Review Manual 15th Edition, page 101, page 102.

NEW QUESTION: 79

A backdoor has been identified that enabled a cyberattack on an organization's systems. Integrating which of the following into the software development life cycle would BEST enable the organization to mitigate similar attacks in the future?

A. Enhanced user acceptance testing (UAT)

B. Separation of duties

C. Customized developer training

D. Vulnerability testing

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 80

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:

Procram.net

A. change activities are documented.

B. the rationale for acceptance is periodically reviewed.

C. the acceptance is aligned with business strategy.

D. compliance with the risk acceptance framework.

Answer: (SHOW ANSWER)

= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.

References =

CISM Review Manual 15th Edition, page 1131

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

NEW QUESTION: 81

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: 82
An organization is performing due diligence when selecting a third party. Which of the following is MOST helpful to reduce the risk of unauthorized sharing of information during this process?
A. Using secure communication channels
B. Establishing mutual non-disclosure agreements (NDAs)
C. Requiring third-party privacy policies
D. Obtaining industry references
Answer: (SHOW ANSWER)
The best option to reduce the risk of unauthorized sharing of information during the due diligence process is B). Establishing mutual non-disclosure agreements (NDAs). This is because NDAs are legal contracts that bind the parties to keep confidential any information that is exchanged or disclosed during the due diligence process. NDAs can help to protect the sensitive data, intellectual property, trade secrets, or business strategies of both the organization and the third party from being leaked, stolen, or misused by unauthorized parties.
NDAs can also specify the terms and conditions for the use, storage, and disposal of the information, as well as the consequences for breaching the agreement.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 70, page 18

NEW QUESTION: 83
Reverse lookups can be used to prevent successful:
A. denial of service (DoS) attacks
B. session hacking
C. phishing attacks
D. Internet protocol (IP) spoofing
Answer: D (LEAVE A REPLY)
Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

NEW QUESTION: 84

What is the BEST way to address vulnerabilities associated with a recent increase in the number of zero-day attacks?

A. Implement USB port control throughout the company.

B. Implement automated antivirus updates.

C. Implement a behavior anomaly detection solution.

D. Develop a patching program.

Answer: (SHOW ANSWER)

Zero-day attacks exploit unknown vulnerabilities for which patches and signatures do not yet exist. Therefore, behavior anomaly detection (C) is the most effective approach because it focuses on abnormal system behavior, not known attack patterns. USB controls (A) address a specific threat vector but do not broadly mitigate zero-day risks. Automated antivirus updates (B) and patching programs (D) are essential baseline controls, but they are reactive and ineffective against unknown exploits. CISM emphasizes a risk-based, layered defense strategy, where advanced detection capabilities are used to identify and respond to emerging threats that bypass traditional controls. Behavior-based detection improves resilience against evolving and unknown attack techniques.

References: ISACA CISM Review Manual (Risk management-threat landscape, control selection, emerging risks); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 85

Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?

A. IT strategy

B. Recovery strategy

C. Risk mitigation strategy

D. Security 'strategy

Answer: (SHOW ANSWER)

NEW QUESTION: 86

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

A. Fallback processes are tested the weekend before changes are made

B. Users are not notified of scheduled system changes

C. A manual rather than an automated process is used to compare program versions.

D. The development manager migrates programs into production

Answer: (SHOW ANSWER)

The change management procedure that is MOST likely to cause concern to the information security manager is the development manager migrating programs into production, because it involves a high-risk activity that could compromise the confidentiality, integrity, and availability of the information systems and data.

Migrating programs into production without proper testing, validation, and approval could introduce errors, vulnerabilities, or conflicts that could affect the performance, functionality, or

security of the systems. Fallback processes are tested the weekend before changes are made, users are not notified of scheduled system changes, and a manual rather than an automated process is used to compare program versions are all acceptable change management procedures that do not pose significant risks to the information security manager. References = CISM Review Manual, 16th Edition, page 3121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1522

NEW QUESTION: 87
Which of the following is the BEST indication of a mature information security program?
A. Security incidents are managed properly.
B. Security spending is below budget.
C. Security resources are optimized.
D. Security audit findings are reduced.
Answer: (SHOW ANSWER)
A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

NEW QUESTION: 88
Relationships between critical systems are BEST understood by
A. evaluating key performance indicators (KPIs)
B. performing a business impact analysis (BIA)
C. developing a system classification scheme
D. evaluating the recovery time objectives (RTOs)
Answer: (SHOW ANSWER)
The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

NEW QUESTION: 89
Which of the following is the PRIMARY reason that an information security manager should restrict the use of generic administrator accounts in a multi-user environment?
A. To prevent unauthorized user access

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

NEW QUESTION: 90
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?
Freecram.net
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: 91
A hacking group has posted an organization's employee data on social media. What should the information security manager do FIRST?
A. Inform the impacted employees.
B. Initiate the incident response process.
C. Escalate to senior management.
D. Engage a forensic analysis team.
Answer: (SHOW ANSWER)
The first action the information security manager should take is to initiate the incident response process (B).
According to CISM incident management principles, once there is confirmed evidence of a security incident- such as employee data being publicly disclosed-the organization must

immediately activate its formal incident response procedures. This ensures that actions are coordinated, evidence is preserved, roles and responsibilities are clear, and regulatory, legal, and communication requirements are handled in a controlled manner.
Informing impacted employees (A), escalating to senior management (C), and engaging forensic experts (D) are all important steps, but they are subsequent actions that occur within the incident response process, not before it. Initiating the incident response process provides the structured framework needed to assess scope, contain damage, meet notification obligations, and determine whether forensic investigation is required.
CISM emphasizes that ad hoc actions taken outside the incident response process increase the risk of miscommunication, legal exposure, and ineffective containment. Activating the process first ensures disciplined execution aligned with governance, legal, and regulatory expectations.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident response lifecycle and escalation ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 92
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. Parallel test
B. Simulation test
C. Structured walk-through
D. Full interruption test
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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: 94

The BEST way to integrate information security governance with corporate governance is to ensure:

A. the information security steering committee monitors compliance with security policies.

B. management teams embed information security into business processes.

C. awareness programs include industry best practice for information security governance.

D. the information security program is included in regular external audits.

Answer: B (LEAVE A REPLY)

The best way to integrate information security governance with corporate governance is for management teams to embed information security into business processes. The CISM Review Manual explains that aligning security objectives and activities with organizational goals and business processes ensures that security is a core part of business operations and strategy, not an isolated activity.

Reference:ISACA CISM Review Manual, 16th Edition, Page 38-39, "Integration of Information Security with Business Processes".

NEW QUESTION: 95

Which of the following is the BEST reason to implement a comprehensive information security management system?

A. To ensure continuous alignment with the organizational strategy

B. To gain senior management support for the information security program

C. To support identification of key risk indicators (KRIs)

D. To facilitate compliance with external regulatory requirements

Answer: (SHOW ANSWER)

According to the CISM Review Manual, 15th Edition, the primary objective of an information security management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks.

References = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

NEW QUESTION: 96

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. Notify the regulatory agency of the incident.

C. Implement mitigating controls.

D. Evaluate the impact to the business.

Answer: (SHOW ANSWER)

NEW QUESTION: 97

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

A. Containment

B. Recovery

C. Escalation

D. Investigation

Answer: (SHOW ANSWER)

NEW QUESTION: 98

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: 99

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

NEW QUESTION: 100
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.

NEW QUESTION: 101
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: 102

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: 103
Which of the following presents the GREATEST challenge to the recovery of critical systems and data following a ransomware incident?
A. Lack of encryption for backup data in transit
B. Undefined or undocumented backup retention policies
C. Ineffective alert configurations for backup operations
D. Unavailable or corrupt data backups
Answer: (SHOW ANSWER)
A ransomware incident is a type of cyberattack that encrypts the victim's data and demands a ransom for its decryption. Ransomware can cause significant disruption and damage to critical systems and data, as well as financial losses and reputational harm. To recover from a ransomware incident, the organization needs to have reliable and accessible backups of its data, preferably in an encrypted format. However, if the backups are unavailable or corrupt, the organization will face a major challenge in restoring its data and operations. Therefore, option D is the most challenging factor for the recovery of critical systems and data following a ransomware incident. References = CISA MS-ISAC Ransomware Guide1, page 9; How to Write an Incident Response Plan for Ransomware Recovery2.

NEW QUESTION: 104
Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?
A. Enterprise risk committee
B. Chief information security officer (CISO)
C. Information security steering committee
D. Data privacy officer (DPO)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
An organization is in the process of defining policies for employee use of social media. It is MOST important for the information security manager to:
A. Assign accountability for monitoring social media
B. Identify security monitoring tools
C. Evaluate risks to the organization
D. Develop security awareness training
Answer: (SHOW ANSWER)
Before drafting or enforcing policies, the first step is to evaluate the risks posed by employee use of social media. This may include data leakage, reputational damage, phishing, and legal liability.

Once risks are identified and understood in the organization's context, policies can be developed that specifically address those risks. Acting prematurely without a risk assessment can lead to overly restrictive or insufficient policies.
"Security policies should be risk-driven. Understanding potential threats and impacts is the foundation for effective policy creation."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Risk-Based Policy Development*

NEW QUESTION: 106
Which of the following would be MOST important to include in a proposal justifying investments for an organization's information security program?
A. Vulnerability scan results
B. Competitor benchmark analysis
C. Previous security budget
D. Business requirements
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Justifying investments in information security requires aligning proposals with business objectives to gain management approval.
A). Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.
B). Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.
C). Previous security budget: Historical data may provide context but does not justify future needs.
D). Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders.
Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 107

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

NEW QUESTION: 108
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: 109
An information security policy was amended recently to support an organization's new information security strategy. Which of the following should be the information security manager's NEXT step?
A. Evaluate the alignment with business strategy
B. Update standards and procedures
C. Review technical controls
D. Refresh the security training program
Answer: (SHOW ANSWER)

NEW QUESTION: 110

Which of the following is the BEST way to enhance training for incident response teams?

A. Perform post-incident reviews.

B. Establish incident key performance indicators (KPIs).

C. Conduct interviews with organizational units.

D. Participate in emergency response activities.

Answer: (SHOW ANSWER)

Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.

References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).

The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

NEW QUESTION: 111

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: 112

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

A. Appropriate communication channels

B. Allocation of needed resources
C. Risk severity and incident priority
D. Response and containment requirements
Answer: (SHOW ANSWER)
The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation.
The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence the allocation of resources, the response and containment requirements, and the communication channels, but they are not the primary purpose of categorization.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

NEW QUESTION: 113
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: 114
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: 115
Which of the following is MOST important for an information security manager to consider when determining whether data should be stored?
A. Data storage limitations
B. Type and nature of data
C. Data protection regulations
D. Business requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 116
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: 117
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: 118
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: 119
Which of the following metrics provides the BEST evidence of alignment of information security governance with corporate governance?
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: 120
When is the BEST time to verify that a production system's security mechanisms meet control objectives?
Freecram.net
A. During quality and acceptance checks
B. On a continuous basis through monitoring activities and automated tooling
C. After remediations recommended by penetration tests have been completed
D. During annual internal and compliance audits
Answer: (SHOW ANSWER)
While audits and assessments provide periodic insights, the best time to verify that security mechanisms meet control objectives is continuously-through monitoring and automation. Continuous monitoring allows the organization to detect misconfigurations, anomalies, or control failures in real-time, significantly improving response capabilities. Modern environments, especially in production systems, require real-time feedback loops to maintain compliance and effectiveness due to rapidly evolving threats and configuration changes.
"Continuous monitoring provides assurance that controls are operating effectively in real time, enabling timely corrective actions."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Control Monitoring*

NEW QUESTION: 121

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

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122

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: 123

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: 124
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: 125
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: 126
A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:
A. incident has been confirmed.
B. incident has been contained.
C. potential incident has been logged.
D. incident has been mitigated.
Answer: (SHOW ANSWER)
= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.
The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset.
References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

NEW QUESTION: 127
Identifying which of the following BEST enables a cyberattack to be contained?
A. The IP address of the computer that launched the attack
B. The segment targeted by the attack
C. The vulnerability exploited by the attack

D. The threat actor that initiated the attack
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?
A. Delegate the management of access permissions to an independent third party.
B. Lock out accounts after a set number of unsuccessful login attempts.
C. Enable multi-factor authentication on user and admin accounts.
D. Review access permissions annually or whenever job responsibilities change
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A risk assessment exercise has identified the threat of a denial of service (DoS) attack Executive management has decided to take no further action related to this risk. The MO ST likely reason for this decision is
A. the risk assessment has not defined the likelihood of occurrence
B. the reported vulnerability has not been validated
C. executive management is not aware of the impact potential
D. the cost of implementing controls exceeds the potential financial losses.
Answer: (SHOW ANSWER)
The most likely reason for executive management to take no further action related to the risk of a denial of service (DoS) attack is that the cost of implementing controls exceeds the potential financial losses. This means that the risk is acceptable or tolerable for the organization, and that the benefits of reducing the risk do not outweigh the costs of applying the controls. This decision is based on a cost-benefit analysis, which is a common technique for evaluating and comparing different risk response options. A cost-benefit analysis considers the following factors:
The estimated impact of the risk, which is the potential loss or damage that the organization may suffer if the risk materializes. The impact can be expressed in quantitative or qualitative terms, such as monetary value, reputation, customer satisfaction, legal liability, etc.
The estimated likelihood of occurrence, which is the probability or frequency that the risk will occur within a given time period. The likelihood can be expressed in numerical or descriptive terms, such as percentage, rating, high, medium, low, etc.
The estimated cost of controls, which is the total amount of resources that the organization needs to invest in order to implement and maintain the controls. The cost can include direct and indirect expenses, such as hardware, software, personnel, training, maintenance, etc.
The estimated benefit of controls, which is the reduction in the impact or likelihood of the risk as a result of implementing the controls. The benefit can be expressed in the same terms as the impact or likelihood, such as monetary value, percentage, rating, etc.
A cost-benefit analysis can be performed using various methods, such as net present value (NPV), return on investment (ROI), internal rate of return (IRR), etc. The general principle is to

compare the cost and benefit of each control option, and select the one that provides the highest net benefit or the lowest net cost. A control option is considered feasible and desirable if its benefit exceeds its cost, or if its cost is lower than the impact of the risk.
In this case, executive management has decided to take no further action related to the risk of a DoS attack, which implies that the cost of implementing controls exceeds the potential financial losses. This could be because the impact or likelihood of the risk is low, or because the cost or complexity of the controls is high, or both. For example, the organization may have a robust backup and recovery system, a diversified network infrastructure, a strong customer loyalty, or a low dependency on online services, which reduce the impact or likelihood of a DoS attack. Alternatively, the organization may face technical, financial, or operational challenges in implementing effective controls, such as firewalls, load balancers, traffic filters, or cloud services, which increase the cost or complexity of the controls. Therefore, executive management may have concluded that the risk is acceptable or tolerable, and that taking no further action is the most rational and economical choice.
The other options are not the most likely reasons for executive management to take no further action related to the risk of a DoS attack, as they indicate a lack of proper risk assessment or validation. The risk assessment should define the likelihood of occurrence and the reported vulnerability should be validated, as these are essential steps for identifying and analyzing the risk. Executive management should be aware of the impact potential, as this is a key factor for evaluating and prioritizing the risk. If any of these options were true, executive management would not have enough information or evidence to make an informed and justified decision about the risk response. References = CISM Review Manual, Chapter 2, pages 67-69 CISM Exam Content Outline | CISM Certification | ISACA, Domain 2, Task 2.2 Information Security Risk Management for CISM - Pluralsight, Module 2, Section 2.3 CISM: Information Risk Management Part 2 from Skillsoft - NICCS, Section 2.4 Executive management may not take action related to a risk if they have determined that the cost of implementing necessary controls to mitigate the risk exceeds the potential financial losses that the organization may incur if the risk were to materialize. In cases such as this, it is important for the information security team to provide the executive team with thorough cost-benefit analysis that outlines the cost of implementing the controls versus the expected losses from the risk.

NEW QUESTION: 130

Of the following, who is BEST positioned to approve specific information security risk treatment options?

A. Risk owner
B. Information security manager
C. Head of risk management
D. Senior management

Answer: (SHOW ANSWER)

The risk owner (A) is best positioned to approve specific risk treatment options because they are accountable for the business process or asset affected by the risk and ultimately bear the consequences of that decision.

CISM clearly distinguishes between roles that advise on risk (e.g., information security manager, risk management function) and those that own and accept risk. Senior management (D) defines risk appetite and tolerance, but day-to-day treatment decisions are delegated to risk owners within those boundaries. Approving treatment options requires an understanding of operational impact, cost, and business value-making the risk owner the appropriate authority.
References: ISACA CISM Review Manual (Risk management-risk ownership, accountability, and risk response); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 131
Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?
A. Implement mitigating actions immediately.
B. Invoke the incident response plan.
C. Inform senior management of the breach.
D. Validate the breach.
Answer: (SHOW ANSWER)
The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions.
Invoking the incident response plan or informing management comes after the breach is validated.
Reference:ISACA CISM Review Manual, 16th Edition, Page 280, "Incident Detection and Validation".

NEW QUESTION: 132
Which of the following should be the KEY consideration when creating an information security communication plan with industry peers?
A. Ensuring information is detailed enough to be of use to other organizations
B. Reducing the costs associated with information sharing by automating the process
C. Balancing the benefits of information sharing with the drawbacks of sharing sensitive information
D. Notifying the legal department whenever incident-related information is shared
Answer: (SHOW ANSWER)

NEW QUESTION: 133
A user reports a stolen personal mobile device that stores sensitive corporate data. Which of the following will BEST minimize the risk of data exposure?
A. Prevent the user from using personal mobile devices.
B. Report the incident to the police.
C. Wipe the device remotely.

D. Remove user's access to corporate data.

Answer: C (LEAVE A REPLY)

Wiping the device remotely is the best option to minimize the risk of data exposure from a stolen personal mobile device. This action will erase all the data stored on the device, including the sensitive corporate data, and prevent unauthorized access or misuse. Wiping the device remotely can be done using enterprise mobility management (EMM) or mobile device management (MDM) tools that allow administrators to remotely manage and secure mobile devices. Alternatively, some mobile devices have built-in features that allow users to wipe their own devices remotely using another device or a web portal.

Preventing the user from using personal mobile devices is not a feasible option, as it may affect the user's productivity and convenience. Moreover, this option does not address the immediate risk of data exposure from the stolen device.

Reporting the incident to the police is a good practice, but it does not guarantee that the device will be recovered or that the data will be protected. The police may not have the resources or the authority to track down the device or access it.

Removing the user's access to corporate data is a preventive measure that can limit the damage caused by a stolen device, but it does not eliminate the risk of data exposure from the data already stored on the device.

The user may have cached or downloaded data that can still be accessed by an attacker even if the user's access is revoked. References = Guidelines for Managing the Security of Mobile Devices in the Enterprise NIST Special Publication, Section
3.1.11, page 3-8

CISM Review Manual, Chapter 3, page 121

Mobile device security - CISM Certification Domain 2: Information Risk Management Video Boot Camp
2019, Section 3.3, 00:03:10

NEW QUESTION: 134

Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?

A. Capability maturity model

B. Vulnerability assessment

C. IT security risk and exposure

D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

A capability maturity model (CMM) is a framework that helps organizations assess and improve their processes and capabilities in various domains, such as software development, project management, information security, and others1. A CMM defines a set of levels or stages that represent the degree of maturity or effectiveness of an organization's processes and capabilities in a specific domain. Each level has a set of criteria or characteristics that an organization must meet to achieve that level of maturity. A CMM also provides guidance and best practices on how

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

NEW QUESTION: 135
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: 136
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*

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137
Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?
A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes
C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards
Answer: (SHOW ANSWER)
A service provider is a third-party supplier that provides IT services or products to an organization. A service provider should comply with the organization's information security requirements, such as policies, standards, procedures, and controls, to ensure the confidentiality,

integrity, and availability of the organization's data and systems. The best way to provide an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements is to have the ability to audit the third-party supplier's IT systems and processes. An audit is a systematic and independent examination of evidence to determine the degree of conformity to predetermined criteria. An audit can verify the effectiveness and efficiency of the service provider's security controls, identify any gaps or weaknesses, and provide recommendations for improvement. An audit can also ensure that the service provider adheres to the contractual obligations and service level agreements (SLAs) with the organization. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a live demonstration of the third-party supplier's security capabilities may not be comprehensive, objective, or reliable. A live demonstration may only show the positive aspects of the service provider's security, but not reveal any hidden or potential issues. A live demonstration may also be subject to manipulation or deception by the service provider.
Option C is not the best answer because third-party security control self-assessment (CSA) results may not be accurate, complete, or consistent. A self-assessment is a process where the service provider evaluates its own security controls against a set of criteria or standards. A self-assessment may be biased, subjective, or incomplete, as the service provider may not disclose or report all the relevant information or issues. A self- assessment may also vary in quality and scope depending on the service provider's expertise, resources, and methodology.
Option D is not the best answer because an independent review report indicating compliance with industry standards may not be sufficient or specific for the organization's information security requirements. An independent review is a process where an external party evaluates the service provider's security controls against a set of industry standards or best practices, such as ISO/IEC 27001, NIST CSF, PCI DSS, etc. An independent review report may provide a general overview of the service provider's security posture, but not address the organization's unique or specific security needs, risks, or expectations. An independent review report may also be outdated, limited, or generic, as the industry standards or best practices may not reflect the current or emerging security threats or trends. References = CISM Review Manual 15th Edition1, pages 257-
258; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 301.
An independent review report indicating compliance with industry standards BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

NEW QUESTION: 138

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

A. To improve awareness of information security

B. To disclose the root cause of the incident

C. To increase goodwill toward the organization

D. To comply with regulations regarding notification

Answer: (SHOW ANSWER)

Complying with regulations regarding notification is the most important reason for an organization to communicate to affected parties that a security incident has occurred, as it helps to avoid legal penalties, fines, or sanctions that may result from failing to notify the relevant authorities, customers, or other stakeholders in a timely and appropriate manner. Additionally, complying with regulations regarding notification may also help to preserve the trust and reputation of the organization, as well as to facilitate the investigation and resolution of the incident.

References = CISM Review Manual 2022, page 3151; CISM Exam Content Outline, Domain 4, Task 4.5

NEW QUESTION: 139

The BEST way to report to the board on the effectiveness of the information security program is to present:

A. peer-group industry benchmarks.

B. a summary of the most recent audit findings.

C. a report of cost savings from process improvements.

D. a dashboard illustrating key performance metrics.

Answer: (SHOW ANSWER)

NEW QUESTION: 140

When developing security processes for handling credit card data on the business unit's information system, the information security manager should FIRST:

Freecram.net

A. review corporate policies regarding credit card information.

B. ensure alignment with industry encryption standards.

C. ensure that systems that handle credit card data are segmented.

D. review industry best practices for handling secure payments.

Answer: (SHOW ANSWER)

NEW QUESTION: 141

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: 142

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: (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: 143

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: 144
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: 145
Which of the following BEST enables an organization to determine what activities and changes have occurred on a system during a cybersecurity incident?
A. Root cause analysis
B. Continuous log monitoring
C. Penetration testing
D. Computer forensics
Answer: (SHOW ANSWER)
Computer forensics (D) best enables an organization to determine what activities occurred and what changes were made to a system during a cybersecurity incident. In CISM incident management, computer forensics focuses on the systematic collection, preservation, analysis, and reconstruction of digital evidence to establish a detailed timeline of events, attacker actions,

data access, and system modifications. This capability is essential for understanding the scope and impact of an incident, supporting legal or regulatory requirements, and preventing recurrence. Continuous log monitoring (B) supports detection and early awareness of suspicious activity, but logs alone may be incomplete, altered, or insufficient to fully reconstruct attacker behavior. Root cause analysis (A) is performed after facts are established and focuses on why an incident occurred, not what exactly happened.
Penetration testing (C) is a proactive security testing activity and is unrelated to incident investigation.
CISM emphasizes that once an incident has occurred, forensic analysis is critical to ensure accurate incident handling, evidence integrity, accountability, and informed remediation decisions.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident investigation and forensics ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

NEW QUESTION: 146
An information security team has confirmed that threat actors are taking advantage of a newly announced critical vulnerability within an application. Which of the following should be done FIRST?
A. Install additional application controls.
B. Notify senior management.
C. Invoke the incident response plan.
D. Prevent access to the application.
Answer: C (LEAVE A REPLY)
According to the NIST SP 800-61 Computer Security Incident Handling Guide1, the first step in responding to a cybersecurity incident is to invoke the incident response plan (IRP), which is a written document that defines the roles, responsibilities, and procedures for dealing with a confirmed or suspected security breach1. The IRP helps the organization to prepare for, detect, analyze, contain, eradicate, recover from, and learn from incidents1. Invoking the IRP ensures that the right personnel and resources are mobilized to effectively deal with the threat and minimize the impact.
References = 1: NIST SP 800-61: 1. Introduction1

NEW QUESTION: 147
What is the PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes?
A. Security incident reporting procedures are followed.
B. Security staff turnover is reduced.
C. Information assets are classified appropriately.
D. Access is granted based on task requirements.
Answer: (SHOW ANSWER)

The PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes is that access is granted based on task requirements. This means that the organization can ensure that the employees have the appropriate level and scope of access to the information assets and systems that they need to perform their duties, and that the access is granted, reviewed, and revoked in accordance with the security policies and standards. This can help to reduce the risk of unauthorized access, misuse, or leakage of information, as well as to comply with the principle of least privilege and the segregation of duties12. Security incident reporting procedures are followed (A) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Security incident reporting procedures are the steps and guidelines that the employees should follow when they detect, report, or respond to a security incident.

Aligning the information security program requirements with the employment and staffing processes can help to ensure that the employees are aware of and trained on the security incident reporting procedures, and that they are enforced and monitored by the management. This can help to improve the effectiveness and efficiency of the incident response process, as well as to comply with the legal and contractual obligations12.

Security staff turnover is reduced (B) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit.

Security staff turnover is the rate at which the security personnel leave or join the organization. Aligning the information security program requirements with the employment and staffing processes can help to reduce the security staff turnover by ensuring that the security roles and responsibilities are clearly defined and communicated, that the security personnel are adequately compensated and motivated, and that the security personnel are evaluated and developed regularly. This can help to retain the security talent and expertise, as well as to reduce the costs and risks associated with the security staff turnover12. Information assets are classified appropriately is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Information asset classification is the process of assigning a security level or category to the information assets based on their value, sensitivity, and criticality to the organization. Aligning the information security program requirements with the employment and staffing processes can help to ensure that the information assets are classified appropriately by establishing the ownership and custody of the information assets, the criteria and methods for the information asset classification, and the roles and responsibilities for the information asset classification. This can help to protect the information assets according to their security level or category, as well as to comply with the regulatory and contractual requirements12. References = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG)

[2022 update]2

NEW QUESTION: 148
An organization has been penalized by regulatory authorities for failing to notify them of a major security breach that may have compromised customer data. Which of the following is MOST likely in need of review and updating to prevent similar penalties in the future?
A. Business continuity plan (BCP)
B. Incident communication plan
C. Incident response training program
D. Information security policies and procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 149
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: 150
Which of the following is the GREATEST benefit resulting from the introduction of data security standards for payment cards?
Freecram.net
A. It helps achieve the holistic protection of information assets in the industry.
B. It deters hackers from committing crimes related to card payments.
C. It optimizes budget allocation for cybersecurity in each organization.
D. It enables a wider range of more sophisticated payment methods.
Answer: (SHOW ANSWER)

The greatest benefit of payment card data security standards is that they drive consistent, industry-wide protection of information assets (A). CISM governance emphasizes that standards such as those for payment cards establish minimum baselines that improve security maturity across the entire ecosystem. They do not eliminate attacks (B), optimize budgets (C), or directly enable new payment methods (D). Instead, they raise the overall level of protection, reduce systemic risk, and support trust in payment systems by ensuring consistent application of fundamental security controls.
References: ISACA CISM Review Manual (Governance-industry standards, baseline security); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 151
An information security manager learns that an existing supplier plans to begin using its recently developed generative AI technology for the same scope of service. A risk assessment was performed on the supplier three months ago with no outstanding findings. Which of the following is the BEST course of action to address the associated risk?
A. Suspend the use of the supplier until a risk assessment of the AI technology has been performed
B. Report the change in risk to senior management
C. Review the results of the previous risk assessment
D. Add an indemnity clause in the contractual agreement at the renewal stage
Answer: (SHOW ANSWER)
Generative AI introduces new risks (e.g., data leakage, model poisoning). These risks were not part of the original assessment, so a fresh risk assessment must be conducted before continuing service.
"When a significant change in third-party operations occurs, it necessitates a reassessment of risk before continuing operations."
- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management* This ensures security, compliance, and operational continuity.

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 152
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: C (LEAVE A REPLY)
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: 153
Which of the following analyses will BEST identify the external influences to an organization's information security?
A. Business impact analysis (BIA)
B. Gap analysis
C. Threat analysis
D. Vulnerability analysis
Answer: C (LEAVE A REPLY)
A threat analysis will best identify the external influences to an organization's information security because it involves identifying and evaluating the sources and likelihood of potential adverse events that could affect the organization's assets, operations, or reputation. External influences include factors such as emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, and threat landscape1. A threat analysis can help the organization to align its information security strategy with its business objectives and risk appetite, and to prioritize and mitigate the most relevant and impactful threats.
A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA does not directly identify the external influences to the organization's information security, but rather the impact of those influences on the organization's continuity and recovery. A gap analysis is a process of

comparing the current state of the organization's information security with a desired or expected state, based on best practices, standards, or frameworks. A gap analysis does not directly identify the external influences to the organization's information security, but rather the areas of improvement or compliance. A vulnerability analysis is a process of identifying and evaluating the weaknesses or flaws in the organization's information systems or processes that could be exploited by threats. A vulnerability analysis does not directly identify the external influences to the organization's information security, but rather the exposure or susceptibility of the organization to those influences. References = CISM Review Manual, 15th Edition, pages 22-232; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.113 Threat analysis is a process that is used to identify and assess the external influences or threats that could potentially affect an organization's information security. It is used to identify potential risks and develop strategies to mitigate or reduce those risks. Threat analysis involves analyzing the environment, identifying potential threats and their potential impacts, and then evaluating the organization's current security measures and developing strategies to address any deficiencies.

NEW QUESTION: 154
Which of the following roles is accountable for ensuring the impact of a new regulatory framework on a business system is assessed?
A. Information security manager
B. Legal representative
C. Senior management
D. Application owner
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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: 156
A common drawback of email software packages that provide native encryption of messages is that the encryption:
A. cannot encrypt attachments
B. cannot interoperate across product domains.
C. has an insufficient key length.
D. has no key-recovery mechanism.
Answer: B (LEAVE A REPLY)
Email software packages that provide native encryption of messages use proprietary algorithms and formats that are not compatible with other email software packages. This means that the encryption cannot interoperate across product domains, and the recipients of encrypted messages must use the same email software package as the sender to decrypt and read the messages. This limits the usability and scalability of native encryption, and may also pose security risks if the encryption algorithms or formats are not well-tested or widely accepted. A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains1234. References = CISM Review Manual 15th Edition, page 206. The Top 10 Email Encryption Solutions In 2023 - Expert Insights2, The Best Email Encryption Services for 2023 | PCMag3, The Top 12 Email Encryption Services for 2023 - Right Inbox4.
A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

NEW QUESTION: 157
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. perform a risk assessment.
B. review the state of security awareness.
C. review information security policies.
D. perform a gap analysis.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, performing a risk assessment is the most important course of action for an information security manager during the due diligence phase of an acquisition, as it helps to identify and evaluate the potential threats, vulnerabilities and impacts that may affect the information assets of the target organization. A risk assessment also provides the basis for performing a gap analysis, reviewing the information security policies and awareness, and developing a remediation plan.

References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.1, page 1411.

NEW QUESTION: 158
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: 159
Which of the following is the BEST indication of an effective disaster recovery planning process?
A. Recovery time objectives (RTOs) are shorter than recovery point objectives (RPOs).
B. Hot sites are required for any declared disaster.
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: 160
An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?
Freecram.net
A. Identify the skill set of the provider's incident response team.
B. Evaluate the provider's audit logging and monitoring controls.
C. Review the provider's incident definitions and notification criteria.
D. Update the incident escalation process.
Answer: (SHOW ANSWER)
When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident

definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. References = CISM Review Manual, 16th Edition, page 1021 Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

NEW QUESTION: 161
ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?
A. Recommend canceling the outsourcing contract.
B. Request an independent review of the provider's data center.
C. Notify affected customers of the data breach.
D. Determine the extent of the impact to the organization.
Answer: (SHOW ANSWER)
The CISO should first determine the extent of the impact to the organization by assessing the nature and scope of the data breach, the type and sensitivity of the data involved, the potential harm to the organization and its customers, and the legal and contractual obligations of the organization and the service provider. This will help the CISO to prioritize the appropriate actions and resources to respond to the incident and mitigate the risks. The other options are possible actions that the CISO may take after determining the impact, depending on the circumstances and the outcomes of the investigation. References = CISM Review Manual 15th Edition, page 2231; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1030

NEW QUESTION: 162
Which of the following BEST enables staff acceptance of information security policies?
A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program
D. Adequate security funding
Answer: (SHOW ANSWER)

= Strong senior management support is the best factor to enable staff acceptance of information security policies, as it demonstrates the commitment and leadership of the organization's top executives in promoting and enforcing a security culture. Senior management support can also help ensure that the information security policies are aligned with the business goals and values, communicated effectively to all levels of the organization, and integrated into the performance evaluation and reward systems. Senior management support can also help overcome any resistance or challenges from other stakeholders, such as business units, customers, or regulators123. References =
1: CISM Review Manual 15th Edition, page 26-274
2: CISM Practice Quiz, question 1102
3: Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, page 5-6

NEW QUESTION: 163
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: 164
Which of the following should be the PRIMARY basis for an information security strategy?
A. The organization's vision and mission
B. Results of a comprehensive gap analysis
C. Information security policies
D. Audit and regulatory requirements
Answer: (SHOW ANSWER)

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

NEW QUESTION: 165
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: 166
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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 167
Which of the following is MOST important to the effectiveness of an information security program?
A. Security metrics
B. Organizational culture
C. IT governance
D. Risk management
Answer: (SHOW ANSWER)
Risk management is the most important factor for the effectiveness of an information security program, as it provides a systematic and consistent approach to identify, assess, treat, and monitor the information security risks that could affect the organization's objectives. Risk management also helps to align the security program with the business strategy, prioritize the security initiatives and resources, and communicate the value of security to the stakeholders. References = CISM Review Manual 2022, page 3071; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.1

NEW QUESTION: 168
Which of the following is the PRIMARY reason for granting a security exception?
A. The risk is justified by the cost to the business.
B. The risk is justified by the benefit to security.
C. The risk is justified by the cost to security.
D. The risk is justified by the benefit to the business.

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

NEW QUESTION: 169
An information security manager has become aware that system administrators are not changing server administrator accounts from the default usernames. A policy has been created and approved by business managers to require these changes. Which of the following should be the information security manager's FIRST course of action?
A. Include the requirement in information security awareness materials
B. Perform a policy compliance assessment
C. Ensure the policy has been communicated to the system administrators
Answer: (SHOW ANSWER)
The first course of action is to ensure the policy has been communicated to the system administrators (C).
CISM governance principles require that policies be formally communicated and understood before enforcement or compliance assessment occurs. Conducting assessments (B) or training (A) is ineffective if administrators are not aware of the policy requirements. Effective governance follows a sequence: approval # communication # implementation # monitoring and enforcement. Communication ensures accountability and supports consistent adoption of security requirements.
References: ISACA CISM Review Manual (Governance-policy lifecycle, communication and enforcement); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 170
An anomaly-based intrusion detection system (IDS) operates by gathering data on:
A. normal network behavior and using it as a baseline lor measuring abnormal activity
B. abnormal network behavior and issuing instructions to the firewall to drop rogue connections
C. abnormal network behavior and using it as a baseline for measuring normal activity
D. attack pattern signatures from historical data
Answer: (SHOW ANSWER)

An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

NEW QUESTION: 171
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: 172
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: 173
Which of the following is MOST important for the successful implementation of an incident response plan?
A. Developing metrics for incident response reporting
B. Developing a RACI chart of response staff functions
C. Ensuring response staff are appropriately trained
D. Establishing an escalation process for the help desk
Answer: (SHOW ANSWER)

NEW QUESTION: 174
Which of the following should be done FIRST when establishing an information security governance framework?
A. Gain an understanding of the business and cultural attributes.
B. Conduct a cost-benefit analysis of the framework.
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: 175
A balanced scorecard MOST effectively enables information security:
A. project management
B. governance.
C. performance.
D. risk management.
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 176
An organization has identified IT failures in a call center application. Of the following, who should own this risk?
A. Chief executive officer (CEO)
B. Information security manager

C. Head of the IT department
D. Head of the call center
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring
Answer: (SHOW ANSWER)
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

NEW QUESTION: 178
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: 179
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: 180
Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?
Freecram.net
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: 181
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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 182
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. Implement compensating controls for the application.

B. Purchase cybersecurity insurance.
C. Discontinue using the application.
D. Accept the risk associated with continued use of the application.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
The PRIMARY consideration when responding to a ransomware attack should be to ensure:
A. backups are available.
B. the most recent patches have been applied.
C. the ransomware attack is contained
D. the business can operate
Answer: (SHOW ANSWER)
Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
* https://www.cisa.gov/stopransomware/ransomware-guide
* https://csrc.nist.gov/Projects/ransomware-protection-and-response
* https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

NEW QUESTION: 184
An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify, What is the BEST way to help ensure similar incidents are identified more quickly in the future?
A. Perform a post-incident review.
B. Implement a SIEM solution.
C. Perform a threat analysis.
D. Establish performance metrics for the team.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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

NEW QUESTION: 186
An organization has multiple data repositories across different departments. The information security manager has been tasked with creating an enterprise strategy for protecting data. Which of the following information security initiatives should be the HIGHEST priority for the organization?
A. Data masking
B. Data retention strategy
C. Data encryption standards
D. Data loss prevention (DLP)
Answer: C (LEAVE A REPLY)
Data encryption standards are the best information security initiative for creating an enterprise strategy for protecting data across multiple data repositories and different departments because they help to ensure the confidentiality, integrity, and availability of data in transit and at rest. Data encryption is a process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt it. Data encryption standards are the rules or specifications that define how data encryption should be performed, such as the type, strength, and mode of encryption, the key management and distribution methods, and the compliance requirements. Data encryption standards help to protect data from unauthorized access, modification, or theft, as well as to meet the regulatory obligations for data privacy and security. Therefore, data encryption standards are the correct answer.
References:
https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data-protection-strategy
https://cloudian.com/guides/data-protection/data-protection-strategy-10-components-of-an-effective-strategy/
https://www.veritas.com/information-center/enterprise-data-protection

NEW QUESTION: 187
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: 188
Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?
A. Available annual budget
B. Cost-benefit analysis of mitigating controls
C. Recovery time objective (RTO)
D. Maximum tolerable outage (MTO)
Answer: (SHOW ANSWER)
Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk events." CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise." CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

NEW QUESTION: 189
A business continuity plan (BCP) should contain:
A. Hardware and software inventories
B. Data restoration procedures
C. Information about eradication activities
D. Criteria for activation
Answer: (SHOW ANSWER)
Criteria for activation are essential to ensure that the BCP is triggered appropriately in response to a disruption.
"The BCP should include clearly defined activation criteria to ensure that plans are invoked when necessary."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Planning* ISACA's practice questions confirm that criteria for activation are core to a BCP's effectiveness.

NEW QUESTION: 190

Which of the following is the BEST course of action when an online company discovers a network attack in progress?

Freecram.net

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: 191
Which of the following should be the FIRST step when performing triage of a malware incident?
A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware
Answer: (SHOW ANSWER)
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 192
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: 193
Which of the following BEST indicates that an information security governance framework has been successfully implemented?
A. The framework aligns internal and external resources.
B. The framework aligns security processes with industry best practices.
C. The framework aligns management and other functions within the security organization.
D. The framework includes commercial off-the-shelf security solutions.
Answer: (SHOW ANSWER)
The best indicator that an information security governance framework has been successfully implemented is A: The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.
The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

NEW QUESTION: 194
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: 195
Which of the following considerations is MOST important when selecting a third-party intrusion detection system (IDS) vendor?
A. The vendor's proposal requires the provider to have a business continuity plan (BCP).
B. The vendor's proposal aligns with the objectives of the organization.
C. The vendor's proposal allows for escrow in the event the third party goes out of business.
D. The vendor's proposal allows for contract modification during technology refresh cycles.
Answer: (SHOW ANSWER)

NEW QUESTION: 196
An information security manager has identified that security risks are not being treated in a timely manner.
Which of the following
A. Provide regular updates about the current state of the risks.
B. Re-perform risk analysis at regular intervals.
C. Assign a risk owner to each risk
D. Create mitigating controls to manage the risks.
Answer: (SHOW ANSWER)
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any

attempts to alter or tamper with the message content. References: https://support.microsoft.com/en-us/office/secure- messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com /searchsecurity/definition/digital-signature

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 197
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: 198
A global organization has outsourced security processes to a service provider by means of a global agreement.
What is the MOST efficient approach to meet country-specific regulatory requirements?
A. Include binding corporate rules into the global agreement

B. Set up a governance organization for each country
C. Review the agreement for each country separately
D. Set up companion agreements for each country
Answer: (SHOW ANSWER)
Binding Corporate Rules (BCRs) are legally enforceable and approved data protection policies used to facilitate compliance across multiple jurisdictions. Incorporating BCRs into a global agreement enables the organization to efficiently manage regulatory obligations across countries.
"Binding corporate rules offer a scalable and consistent mechanism to address cross-border compliance in global outsourcing agreements."
- CISM Review Manual 15th Edition, Chapter 1: Governance, Section: Cross-Border Data Protection Considerations* Creating separate agreements per country is inefficient and complex compared to centralized BCR-based governance.

NEW QUESTION: 199
Which of the following backup methods requires the MOST time to restore data for an application?
A. Full backup
B. Incremental
C. Differential
D. Disk mirroring
Answer: (SHOW ANSWER)
= An incremental backup method only backs up the data that has changed since the last backup, whether it was a full or an incremental backup. This method requires the least amount of time and storage space for backup, but it requires the most time to restore data for an application. To restore data from an incremental backup, the latest full backup and all the subsequent incremental backups are needed. A full backup method backs up all the data in a system or an application at a point in time. This method requires the most amount of time and storage space for backup, but it requires the least time to restore data for an application. To restore data from a full backup, only the latest full backup is needed. A differential backup method backs up the data that has changed since the last full backup. This method requires more time and storage space for backup than the incremental method, but less than the full backup method. It also requires less time to restore data for an application than the incremental method, but more than the full backup method. To restore data from a differential backup, the latest full backup and the latest differential backup are needed. A disk mirroring method creates an exact copy of a disk on another disk in real time. This method provides the highest level of availability and fault tolerance, but it also requires twice the amount of disk space. To restore data from a disk mirroring method, the mirrored disk can be used as the primary disk in case of a failure. References = CISM Review Manual 15th Edition, page 201-202.
The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the

application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

NEW QUESTION: 200

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

Freecram.net

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

NEW QUESTION: 201

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: 202

Which of the following is the GREATEST challenge when developing key risk indicators (KRIs)?
A. Limiting the number of KRIs
B. Comprehensively reporting on KRIs
C. Aggregating common KRIs
D. Linking KRIs to specific risks
Answer: (SHOW ANSWER)

The biggest challenge is linking KRIs to specific risks to ensure that they accurately measure and signal potential exposures. If KRIs aren't directly connected to real risks, they won't effectively support risk management efforts.
"A key challenge in developing KRIs is ensuring that they are directly linked to specific risks to provide meaningful and actionable insights."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Key Risk Indicators (KRIs)* ISACA's practice questions highlight the importance of clear linkage for effective risk measurement.

NEW QUESTION: 203
Which of the following is the BEST way to determine if an information security profile is aligned with business requirements?
A. Review the key performance indicator (KPI) dashboard
B. Review security-related key risk indicators (KRIs)
C. Review control self-assessment (CSA) results
D. Review periodic security audits
Answer: (SHOW ANSWER)
Security-related KRIs are metrics that measure the effectiveness of the information security profile in achieving the business objectives and managing the risks. Reviewing security-related KRIs can help to determine if the information security profile is aligned with business requirements, as they reflect the security performance and outcomes that are relevant for the business. Reviewing other options, such as KPIs, CSAs, or audits, may provide some insights into the security status, but they are not the best way to assess the alignment with business requirements, as they may not capture the business context and goals adequately.
References:
* https://www.nist.gov/cyberframework/examples-framework-profiles
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/accountability-for-information- security-roles-and-responsibilities-part-1
* https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea- top-down-approach

NEW QUESTION: 204
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: 205
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: 206
Which of the following roles is MOST appropriate to determine access rights for specific users of an application?
A. Data owner
B. Data custodian
C. System administrator
D. Senior management
Answer: (SHOW ANSWER)
The data owner is the most appropriate role to determine access rights for specific users of an application because they have legal rights and complete control over data elements4. They are also responsible for approving data glossaries and definitions, ensuring the accuracy of information, and supervising operations related to data quality5. The data custodian is responsible for the safe custody, transport, and storage of the data and implementation of business rules, but not for determining access rights4. The system administrator is responsible for managing the security and storage infrastructure of data sets according to the organization's data

governance policies, but not for determining access rights5. Senior management is responsible for setting the strategic direction and priorities for data governance, but not for determining access rights5.
References: 5 https://www.cpomagazine.com/cyber-security/data-owners-vs-data-stewards-vs-data- custodians-the-3-types-of-data-masters-and-why-you-should-employ-them/ 4 https://cloudgal42.com/data- privacy-difference-between-data-owner-controller-and-data-custodian-processor/

NEW QUESTION: 207
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: 208
Which of the following is established during the preparation phase of an incident response plan?
A. Recovery time objectives (RTOs)
B. Chain of custody procedures
C. Mean time to respond (MTTR)
D. Stakeholder communication plan
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which of the following should an information security manager do FIRST upon confirming a privileged user's unauthorized modifications to a security application?
A. Report the risk associated with the policy breach.
B. Enforce the security configuration and require the change to be reverted.
C. Implement compensating controls to address the risk.
D. Implement a privileged access management system.
Answer: (SHOW ANSWER)
The first thing that an information security manager should do upon confirming a privileged user's unauthorized modifications to a security application is to enforce the security configuration and require the change to be reverted. This is because the unauthorized modification may have compromised the security of the application and the data it protects, and may have violated the security policies and standards of the organization. By enforcing the security configuration and requiring the change to be reverted, the information security manager can restore the security posture of the application and prevent further unauthorized modifications.
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 monitor and review the security configuration of information systems 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: "Enforcing the security configuration and requiring the change to be reverted is the correct answer because it is the most immediate and effective action to address the unauthorized modification and to maintain the security of the application" (p. 63). Additionally, the Effective Interactive Privileged Access Review article from the ISACA Journal 2018 states that "any

unauthorized changes to the production environment should be reverted back to the original state and the incident should be reported to the appropriate authority" (p. 4)1.

NEW QUESTION: 210

For an e-business that requires high availability, which of the following design principles is BEST?

A. Manual failover to the website of another e-business that meets the user's needs

B. A single point of entry allowing transactions to be received and processed quickly

C. Intelligent middleware to direct transactions from a downed system to an alternative

D. Availability of an adjacent cold site and a standby server with mirrored copies of critical data

Answer: (SHOW ANSWER)

Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention. "Middleware solutions can provide automated failover capabilities, improving system resilience and availability."

- CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section:

Availability and Resilience*

Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

NEW QUESTION: 211

An organization has identified an increased threat of external brute force attacks in its environment. Which of the following is the MOST effective way to mitigate this risk to the organization's critical systems?

A. Implement multi-factor authentication.

B. Increase the frequency of log monitoring and analysis.

C. Implement a security information and event management system (SIEM),

D. Increase the sensitivity of intrusion detection systems (IDSs).

Answer: (SHOW ANSWER)

A brute force attack is a type of cyberattack that attempts to gain unauthorized access to an account, file, or other protected information by trying different combinations of usernames and passwords until finding the correct one. Brute force attacks can be very effective if the target system has weak or default passwords, or if the attacker has access to a large number of potential credentials. To mitigate this risk, an organization should implement multi-factor authentication (MFA) for its critical systems. MFA is a security method that requires users to provide more than one piece of evidence to verify their identity before accessing a system or service.

For example, MFA can involve using a password in addition to a code sent to a phone or email, or using a biometric factor such as a fingerprint or face scan. MFA can significantly reduce the impact of brute force attacks by making it harder for attackers to guess or obtain valid credentials, and by increasing the time and effort required for them to compromise the system. References =

CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 212
Which of the following is the MOST critical activity for an information security manager to perform periodically throughout the term of a contract with an outsourced third party?
A. Participatory disaster recovery testing
B. Comprehensive risk assessments
C. Service level agreement (SLA) updates
D. Financial alignment reviews
Answer: (SHOW ANSWER)
Performing comprehensive risk assessments (B) throughout the life of a third-party contract is the most critical activity because risk posture changes over time due to evolving threats, business changes, or control degradation. CISM emphasizes that third-party risk is not static and must be continuously assessed to ensure ongoing alignment with risk appetite. Disaster recovery testing (A) and SLA updates (C) are important but limited in scope. Financial reviews (D) focus on cost rather than security risk. Periodic risk assessments enable timely identification of new risks and ensure appropriate mitigation or escalation.
References: ISACA CISM Review Manual (Governance-third-party risk lifecycle management); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 213
Which of the following would BEST enable the timely execution of an incident response plan?
A. The introduction of a decision support tool
B. Definition of trigger events
C. Clearly defined data classification process
D. Centralized service desk
Answer: (SHOW ANSWER)

Definition of trigger events is the best way to enable the timely execution of an incident response plan because it helps to specify the conditions or criteria that initiate the incident response process. Trigger events are predefined scenarios or indicators that signal the occurrence or potential occurrence of a security incident, such as a ransomware attack, a data breach, a denial-of-service attack, or an unauthorized access attempt.
Definition of trigger events helps to ensure that the incident response team is alerted and activated as soon as possible, as well as to determine the appropriate level and scope of response based on the severity and impact of the incident. Therefore, definition of trigger events is the correct answer.
References:
* https://www.atlassian.com/incident-management/kpis/common-metrics
* https://www.varonis.com/blog/incident-response-plan/
* https://holierthantao.com/2023/05/03/minimizing-disruptions-a-comprehensive-guide-to-incident-response-planning-and-execution/

NEW QUESTION: 214
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: 215
An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?
A. Focus the review on the infrastructure with the highest risk
B. Review controls listed in the vendor contract
C. Determine whether the vendor follows the selected security framework rules
D. Review the vendor's security policy

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

NEW QUESTION: 216
An organization is outsourcing a business function to an external vendor. Which of the following BEST enables management to ensure the vendor continuously complies with security requirements stated in the master contract?
A. Organize a training program for the vendor on the organization's security requirements.
B. Conduct periodic reviews of the vendor's third-party accredited assessments.
C. Establish the right-to-audit security controls at the vendor site.
D. Conduct periodic re-approval of security clauses in the master contract.
Answer: (SHOW ANSWER)
The best way to ensure continuous compliance with security requirements is to conduct periodic reviews of the vendor's third-party accredited assessments (B). From a CISM governance and third-party risk management perspective, ongoing assurance is critical when business-critical functions are outsourced.
Independent third-party assessments (such as SOC reports or equivalent accredited reviews) provide objective, repeatable, and evidence-based validation that security controls are not only defined but are operating effectively over time.
Training programs (A) improve awareness but do not provide assurance of compliance. Establishing right-to- audit clauses (C) is an important contractual safeguard, but it is typically reactive or periodic, not a continuous monitoring mechanism. Re-approving contract clauses (D) ensures contractual relevance but does not validate actual control effectiveness.
CISM emphasizes that continuous vendor compliance is best achieved through independent assurance mechanisms integrated into ongoing vendor oversight, enabling management to monitor control effectiveness, identify emerging risks, and take timely corrective action. Periodic

review of accredited third-party assessments supports governance transparency, accountability, and alignment with the organization's risk appetite.
References:
ISACA CISM Review Manual, Information Security Governance - third-party risk management and continuous assurance ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 217
An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy, A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:
A. the chief risk officer (CRO).
B. business senior management.
C. the information security manager.
D. the compliance officer.
Answer: (SHOW ANSWER)
Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.
The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The information security manager is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation,

and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

NEW QUESTION: 218
Who has the PRIMARY authority to decide if additional risk treatments are required to mitigate an identified risk?
A. Information security manager
B. IT risk manager
C. Internal auditor
D. Risk owner
Answer: D (LEAVE A REPLY)
The risk owner is the person who has the authority and accountability to make decisions about the risk, including whether to accept, avoid, transfer, or mitigate it. The risk owner is also responsible for implementing and monitoring the risk treatment plan and reporting on the risk status. The risk owner is usually the business process owner or the information owner of the asset affected by the risk. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2.

NEW QUESTION: 219
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: 220

Which of the following tools would be MOST helpful to an incident response team?

A. Intrusion detection system (IDS)
B. Endpoint detection and response (EDR) solution
C. User and entity behavior analytics
D. Vulnerability scanning tools
Answer: (SHOW ANSWER)
An endpoint detection and response (EDR) solution provides advanced visibility, detection, and response capabilities at the endpoint level, which are critical for investigating and responding to incidents.
"EDR solutions help identify, investigate, and respond to threats on endpoints quickly, making them vital for incident response teams."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Tools and Technologies for Incident Response* ISACA's practice questions highlight EDR as the most helpful tool for comprehensive incident analysis and response.

NEW QUESTION: 221
The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:
A. the internal audit manager.
B. the information security officer.
C. the steering committee.
D. the board of directors.
Answer: (SHOW ANSWER)
The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the

organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework. References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 222
Which of the following should be updated FIRST when aligning the incident response plan with the corporate strategy?
A. Disaster recovery plan (DRP)
B. Incident notification plan
C. Risk response scenarios
D. Security procedures
Answer: (SHOW ANSWER)
The answer to the question is C. Risk response scenarios. This is because risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents, such as cyberattacks, natural disasters, or data breaches. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization, and guides the decision- making and resource allocation processes. By aligning the risk response scenarios with the corporate strategy, the organization can ensure that the incident response plan supports the achievement of the desired outcomes and benefits, and minimizes the impact and disruption to the business operations and performance.
Risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2111; CISM domain 4:
Information security incident management [2022 update] | Infosec2; A Guide to Effective Incident Management Communications3

NEW QUESTION: 223
Which of the following is the MOST important issue in a penetration test?
A. Having an independent group perform the test
B. Obtaining permission from audit
C. Performing the test without the benefit of any insider knowledge
D. Having a defined goal as well as success and failure criteria
Answer: (SHOW ANSWER)
The most important issue in a penetration test is having a defined goal as well as success and failure criteria.

A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach, as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

NEW QUESTION: 224
Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?
A. It eliminates the need for the business to perform testing.
B. It transfers the risk associated with recovery to a third party.
C. It eliminates the need to maintain offsite facilities.
D. It lowers the annual cost to the business.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 225
Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?
A. The risks are entered in the organization's risk register.
B. The risks are reported to the business unit's senior management.
C. The risks are escalated to the IT department for remediation.
D. The risks are communicated to the central risk function.
Answer: (SHOW ANSWER)
Entering identified risks into the organization's risk register ensures that they are documented, tracked, assigned, and addressed. Without recording in the risk register, there's no formal mechanism to manage, treat, or monitor the risk.

"The risk register is the central repository for tracking all known risks, their status, and treatment plans."
- CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Risk Response and Risk Register*

NEW QUESTION: 226
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. Monthly metrics
B. Counts of information security incidents
C. Audit reports
D. Updated risk assessments
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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 227
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: 228
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: 229
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: 230
Which of the following should be done FIRST after a ransomware incident has been successfully contained?
Freecram.net

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

NEW QUESTION: 231
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: 232
In the context of developing an information security strategy, which of the following provides the MOST useful input to determine the or
A. Security budget
B. Risk register
C. Risk score
D. Laws and regulations
Answer: (SHOW ANSWER)
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References: https://www.isaca.

org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with- business-goals-and-objectives

NEW QUESTION: 233
Which of the following is the BEST tool to monitor the effectiveness of information security governance?
A. Key performance indicators (KPIs)
B. Balanced scorecard
C. Business impact analysis (BIA)
D. Risk profile
Answer: (SHOW ANSWER)
Key performance indicators (KPIs) are the best tool to monitor the effectiveness of information security governance because they are quantifiable and measurable metrics that reflect the achievement of the information security objectives and the alignment of the information security strategy with the business goals.
KPIs can help to evaluate the performance, efficiency, quality, and value of the information security processes and activities, and to identify the areas of improvement or adjustment. KPIs can also provide feedback to the management and the stakeholders on the status and progress of the information security governance. Some examples of KPIs for information security governance are: percentage of compliance with security policies and standards, number and severity of security incidents, return on security investment, and maturity level of information security capabilities12.
A balanced scorecard is a strategic management tool that translates the vision and mission of the organization into four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help to align the information security strategy with the business strategy, but it is not a tool to monitor the effectiveness of information security governance. A balanced scorecard can include KPIs as part of its measurement system, but it is not a substitute for KPIs13.
A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA can help to identify the critical assets, dependencies, recovery priorities, and recovery objectives for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A BIA is a one-time or periodic activity, not a continuous monitoring process14.
A risk profile is a representation of the organization's exposure to various types of risks, such as operational, financial, strategic, or reputational. A risk profile can help to identify the sources, likelihood, and impact of potential threats to the organization's assets and objectives, and to determine the risk appetite and tolerance for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A risk profile is a snapshot of the organization's risk posture at a given point in time, not a dynamic monitoring tool15. References =

CISM Review Manual, 16th Edition, pages 23-241; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.122; CISM Review Questions, Answers & Explanations Database, Question ID 10093; CISM Review Questions, Answers & Explanations Database, Question ID 10104; CISM Review Questions, Answers & Explanations Database, Question ID 10115

NEW QUESTION: 234
Which of the following has the MOST influence on the information security investment process?
A. IT governance framework
B. Information security policy
C. Security key performance indicators (KPIs)
D. Organizational risk appetite
Answer: (SHOW ANSWER)

NEW QUESTION: 235
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: 236
Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness program?
A. Percentage of employee computers and devices infected with malware
B. Percentage of employees who regularly attend security training
C. Number of security incidents reported to the help desk

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

NEW QUESTION: 237
Several critical systems have been compromised with malware. Which of the following is the BEST strategy to eradicate this incident?
A. Perform malware scanning
B. Reimage the systems
C. Block access to the impacted systems
D. Perform a vulnerability assessment
Answer: (SHOW ANSWER)
Reimaging the systems (B) is the most reliable method to eradicate malware because it ensures complete removal of malicious code, including hidden persistence mechanisms. Malware scanning (A) may miss advanced threats, while blocking access (C) is a containment action, not eradication. Vulnerability assessments (D) help identify weaknesses but do not remove existing malware. CISM incident management guidance prioritizes thorough eradication to prevent reinfection and restore system integrity.
References: ISACA CISM Review Manual (Incident management-eradication strategies); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 238
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: 239
To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?
A. Gap analysis results
B. Level of residual risk
C. Level of risk treatment
D. Configuration parameters
Answer: (SHOW ANSWER)

Level of residual risk is the amount of risk that remains after applying risk treatment options, such as avoidance, mitigation, transfer, or acceptance. The information security manager should compare the level of residual risk with the organization's risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its objectives. The comparison will help to determine whether the risk treatment options are sufficient, excessive, or inadequate, and whether further actions are needed to align the risk level with the risk appetite.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 49: "Residual risk is the risk that remains after risk treatment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 43: "Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value." CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "The information security manager should compare the residual risk with the risk appetite and determine whether the risk treatment options are sufficient, excessive, or inadequate."

NEW QUESTION: 240

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?

Freecram.net

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: 241
From an information security perspective, legal issues associated with a transborder flow of technology- related items are MOST often
A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.
Answer: (SHOW ANSWER)
Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context

because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. References: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on- transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 242
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: 243

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: 244
A new type of ransomware has infected an organization's network. Which of the following would have BEST enabled the organization to detect this situation?
A. Monitoring of anomalies in system behavior
B. Use of integrated patch deployment tools
C. Periodic information security training for end users
D. Regular review of the threat landscape
Answer: (SHOW ANSWER)

NEW QUESTION: 245
Which of the following is the responsibility of a risk owner?
A. Implementing risk treatment plan activities with control owners
B. Evaluating control effectiveness
C. Approving risk treatment plans
D. Approving the selection of risk mitigation measures
Answer: (SHOW ANSWER)
A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk.
While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

NEW QUESTION: 246

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: 247

Which of the following is the PRIMARY responsibility of the information security function when an organization adopts emerging technologies?

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

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

Requirement for regular information security awareness B. Right-to-audit clause C. Service level agreement (SLA) D. Requirement to comply with corporate security policy Answer: (Refer to the Information Security Manager (CISM) documents and learning resources by ISACA available at https://store.isaca.org/s/store#
/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles to verify the answer of the following questions very carefully.) Use the following format please: **Verified answer** = (From CISM Manual or related resources) **Very Short Explanation** = (From CISM Manual or related resources) **References** = (From CISM Manual or related resources) ==========

NEW QUESTION: 248
In order to gain organization-wide support for an information security program, which of the following is MOST important to consider?
A. Maturity of the security policy
B. Clarity of security roles and responsibilities
C. Corporate culture
D. Corporate risk framework
Answer: (SHOW ANSWER)
Corporate culture is the most important factor to consider when trying to gain organization-wide support for an information security program because it reflects the values, beliefs, and behaviors of the organization and its members. Corporate culture influences how the organization perceives, prioritizes, and responds to information security risks and issues, and how it adopts and implements information security policies and practices. By understanding and aligning with the corporate culture, the information security manager can communicate the benefits and value of the information security program, and foster a positive and collaborative security culture across the organization.
References: The CISM Review Manual 2023 states that "corporate culture is the set of shared values, beliefs, and behaviors that characterize the organization and its members" and that "corporate culture affects how the organization views and manages information security risks and issues, and how it supports and implements information security policies and practices" (p. 81). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Corporate culture is the correct answer because it is the most important factor to consider when trying to gain organization-wide support for an information security program, as it reflects the values, beliefs, and behaviors of the organization and its members, and influences how they perceive, prioritize, and respond to information security risks and issues, and how they adopt and implement information security policies and practices" (p. 23). Additionally, the article Building a Culture of Security from the ISACA Journal 2019 states that "corporate culture is the key factor that determines the success or failure of an information security program" and that "corporate culture can be either an enabler or a barrier for information security, depending on how well it aligns with the information security objectives, values, and practices of the organization" (p. 1)

NEW QUESTION: 249
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: 250
The BEST way to identify the risk associated with a social engineering attack is to:
A. monitor the intrusion detection system (IDS),
B. review single sign-on (SSO) authentication lags.
C. test user knowledge of information security practices.
D. perform a business risk assessment of the email filtering system.
Answer: (SHOW ANSWER)
The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.
Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors

network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.
Reviewing single sign-on (SSO) authentication lags (B) is not a relevant way to identify the risk associated with a social engineering attack. SSO is a method of authentication that allows users to access multiple applications or systems with one set of credentials. Authentication lags are delays or failures in the authentication process that may affect the user experience or performance. However, authentication lags are not directly related to social engineering attacks, as they do not indicate the user's knowledge of information security practices, nor the attacker's attempts or success in compromising the user's credentials or access.
Performing a business risk assessment of the email filtering system (D) is also not a relevant way to identify the risk associated with a social engineering attack. An email filtering system is a system that scans, filters, and blocks incoming or outgoing emails based on predefined rules or criteria, such as spam, viruses, or phishing. A business risk assessment is a process that evaluates the potential threats, vulnerabilities, and impacts to the organization's business objectives, processes, and assets. However, performing a business risk assessment of the email filtering system does not address the risk associated with a social engineering attack, as it only focuses on the technical aspects and performance of the system, not the human factors and behavior of the users.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, Subsection: Threat Identification, page 87-881

NEW QUESTION: 251
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: 252
Which of the following is the MOST effective way to determine the alignment of an information security program with the business strategy?
A. Evaluate the results of business continuity testing.
B. Review key performance indicators (KPIs).
C. Evaluate the business impact of incidents.
D. Engage business process owners.
Answer: (SHOW ANSWER)
The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.
Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

NEW QUESTION: 253
Which of the following is MOST important for the improvement of a business continuity plan (BCP)?
A. Implementing an IT resilience solution
B. Implementing management reviews
C. Incorporating lessons learned
D. Documenting critical business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 254
The MOST important information for influencing management's support of information security is:
A. an demonstration of alignment with the business strategy.
B. An identification of the overall threat landscape.
C. A report of a successful attack on a competitor.
D. An identification of organizational risks.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 255
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. Review the incident management procedures.
B. Remove the steps from the incident management procedures.
C. Provide additional training to the incident response team.
D. Interview the incident response team.
Answer: (SHOW ANSWER)

NEW QUESTION: 256
Which of the following documents should contain the INITIAL prioritization of recovery of services?
A. IT risk analysis
B. Threat assessment
C. Business impact analysis (BIA)
D. Business process map
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is the document that should contain the initial priori-tization of recovery of services. A BIA is a process of identifying and analyzing the po-tential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:
*Identifying the critical business functions and processes that support the organization's mission and objectives.

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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 257
An organization is planning to engage a third-party service provider to develop custom software. Which of the following would help to provide the GREATEST assurance of software security?
A. Security training for the service provider's software development staff

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

NEW QUESTION: 258
A business unit recently integrated the organization's new strong password policy into its business application which requires users to reset passwords every 30 days. The help desk is now flooded with password reset requests. Which of the following is the information security manager's BEST course of action to address this situation?
A. Conduct a business impact analysis (BIA).
B. Continue to enforce the policy.
C. Provide end-user training.
D. Escalate to senior management.
Answer: (SHOW ANSWER)

NEW QUESTION: 259
The PRIMARY reason for creating a business case when proposing an information security project is to:
A. articulate inherent risks.
B. provide demonstrated return on investment (ROI).
C. establish the value of the project in relation to business objectives.
D. gain key business stakeholder engagement.
Answer: (SHOW ANSWER)
The primary reason for creating a business case when proposing an information security project is to establish the value of the project in relation to the business objectives and to justify the investment required. A business case should demonstrate how the project aligns with the organization's strategy, goals, and mission, and how it supports the business processes and

functions. A business case should also include the expected benefits, costs, risks, and alternatives of the project, and provide a clear rationale for choosing the preferred option. References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 260

Which of the following is MOST important to include in security incident escalation procedures?

A. Key objectives of the security program

B. Recovery procedures

C. Notification criteria

D. Containment procedures

Answer: (SHOW ANSWER)

The most important thing to include in security incident escalation procedures is notification criteria. This is because notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. Notification criteria help to ensure that the appropriate stakeholders are aware of the incident and can take the necessary actions to respond, mitigate, and recover from it. Notification criteria also help to comply with legal and regulatory requirements for reporting incidents to external parties, such as customers, authorities, or media.

Notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. (From CISM Manual or related resources)

References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2121; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 1, page 1

NEW QUESTION: 261

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: 262
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: 263
Which of the following is MOST important when responding to a major security incident?
A. Contacting forensic investigators
B. Following the escalation process
C. Notifying law enforcement
D. Identifying the indicators of compromise
Answer: (SHOW ANSWER)
Following the escalation process ensures that the incident is managed in accordance with established protocols, involving the right stakeholders and prioritizing the incident appropriately. "Following the escalation process is critical to ensure that incidents are handled appropriately and that the right personnel are engaged at the right time."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Escalation Procedures* ISACA practice questions highlight that proper escalation is vital to ensure incidents are managed effectively and consistently.

NEW QUESTION: 264
Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site
Answer: C (LEAVE A REPLY)
= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. References = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 792 Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 265
Which of the following would BEST guide the development and maintenance of an information security program?
A. A business impact assessment
B. A comprehensive risk register
C. An established risk assessment process
D. The organization's risk appetite
Answer: (SHOW ANSWER)
According to the CISM Manual, the organization's risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives1. The organization's risk appetite should guide the development and maintenance of an information security program, as it determines the level of security controls, resources, and activities that are needed to protect the organization's assets and operations1.
The CISM Manual states that "the information security program should be aligned with the organization's risk appetite, which reflects its tolerance for risk and its strategic objectives" (IR 8288A)1. The information security program should also consider other factors that influence the organization's risk appetite, such as its mission, vision, values, culture, stakeholders, regulations, standards, guidelines, and best practices1.
The CISM Manual also provides guidance on how to develop and maintain an information security program based on the organization's risk appetite. It recommends using a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that affect the organization's information assets1. It also suggests using a framework or model that supports the

development of an information security program based on the organization's risk appetite (e.g., ISO/IEC 27001)1.
References: 1: IR 8288A - Information Security Program Development | CSRC NIST

NEW QUESTION: 266
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 is comprised of representatives from senior management.
D. The committee uses a risk management framework.
Answer: (SHOW ANSWER)

NEW QUESTION: 267
Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?
A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk
Answer: (SHOW ANSWER)
Communicating the residual risk is the best way to facilitate an information security manager's efforts to obtain senior management commitment for an information security program. The residual risk is the level of risk that remains after applying the security controls and mitigation measures. The residual risk reflects the effectiveness and efficiency of the information security program, as well as the potential impact and exposure of the organization. The information security manager should communicate the residual risk to the senior management in a clear, concise, and relevant manner, using quantitative or qualitative methods, such as risk matrices, heat maps, dashboards, or reports. The communication of the residual risk should also include the comparison with the inherent risk, which is the level of risk before applying any security controls, and the risk appetite, which is the level of risk that the organization is willing to accept. The communication of the residual risk should help the senior management to understand the value and performance of the information security program, as well as the need and justification for further investment or improvement. Presenting evidence of inherent risk, reporting the security maturity level, and presenting compliance requirements are all important aspects of the information security program, but they are not the best ways to obtain senior management commitment. These aspects may not directly demonstrate the benefits or outcomes of the information security program, or they may not align with the business objectives or priorities of the organization. For example, presenting evidence of inherent risk may show the potential threats and vulnerabilities that the organization faces, but it may not indicate how the information security program addresses or reduces them. Reporting the security maturity level may show the progress

and status of the information security program, but it may not relate to the risk level or the business impact. Presenting compliance requirements may show the legal or regulatory obligations that the organization must fulfill, but it may not reflect the actual security needs or goals of the organization. Therefore, communicating the residual risk is the best way to obtain senior management commitment for an information security program, as it shows the results and value of the information security program for the organization. References = CISM Review Manual 2023, page 41 1; CISM Practice Quiz 2

NEW QUESTION: 268
Which of the following is the BEST approach for data owners to use when defining access privileges for users?
A. Define access privileges based on user roles.
B. Adopt user account settings recommended by the vendor.
C. Perform a risk assessment of the users' access privileges.
D. Implement an identity and access management (IDM) tool.
Answer: (SHOW ANSWER)
This approach is the best because it ensures that users have the minimum level of access required to perform their job functions, which reduces the risk of unauthorized access or misuse of data. User roles are defined based on the business needs and responsibilities of the users, and they can be easily managed and audited.
References: The CISM Review Manual 2023 states that "the data owner is responsible for defining the access privileges for each user role" and that "the data owner should ensure that the principle of least privilege is applied to all users" (p. 82). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Defining access privileges based on user roles is the best approach because it allows the data owner to assign the minimum level of access required for each role and to review and update the roles periodically" (p. 23).

NEW QUESTION: 269
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. Perform a risk assessment
B. Perform a gap analysis
C. Review information security policies
D. Review the state of security awareness
Answer: (SHOW ANSWER)
During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.
"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence
ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

NEW QUESTION: 270

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

Freecram.net

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

NEW QUESTION: 271
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."

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 272
An information security team must obtain approval from the information security steering committee to implement a key control. Which of the following is the MOST important input to assist the committee in making this decision?
A. Security architecture
B. Business case
C. Risk assessment
D. IT strategy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 273
Which of the following processes is MOST important for the success of a business continuity plan (BCP)?
A. Including the board and senior management in plan reviews
B. Involving all stakeholders in testing and training
C. Scheduling periodic internal and external audits
D. Maintaining copies of the plan at the primary and recovery sites
Answer: (SHOW ANSWER)

NEW QUESTION: 274
Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?
A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.

D. Identify recovery time objectives (RTOs).

Answer: A (LEAVE A REPLY)

= Developing the test plan is the task that should be performed once a disaster recovery plan (DRP) has been developed. The test plan is a document that describes the objectives, scope, methods, and procedures for testing the DRP. The test plan should also define the roles and responsibilities of the test team, the test scenarios and criteria, the test schedule and resources, and the test reporting and evaluation. The purpose of testing the DRP is to verify its effectiveness, identify any gaps or weaknesses, and improve its reliability and usability. Testing the DRP also helps to increase the awareness and readiness of the staff and stakeholders involved in the disaster recovery process. Analyzing the business impact, defining response team roles, and identifying recovery time objectives (RTOs) are all tasks that should be performed before developing the DRP, not after. These tasks are part of the business continuity planning (BCP) process, which aims to identify the critical business functions and assets, assess the potential threats and impacts, and determine the recovery strategies and requirements. The DRP is a subset of the BCP that focuses on restoring the IT systems and services after a disaster. Therefore, the DRP should be based on the results of the BCP process, and tested after it has been developed. References = CISM Review Manual 2023, page 218 1; CISM Practice Quiz 2

NEW QUESTION: 275

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: B (LEAVE A REPLY)

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: 276
When selecting metrics to monitor the effectiveness of an information security program, it is MOST important for an information security manager to:
A. leverage industry benchmarks.
B. consider the strategic objectives of the program.
C. identify the program's risk and compensating controls.
D. consider the organization's business strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 277
Which of the following BEST enables an incident response team to determine appropriate actions during an initial investigation?
A. Historical data from past incidents
B. Procedures for incident triage
C. Feedback from affected departments
D. Technical capabilities of the team
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Which of the following security initiatives should be the FIRST step in helping an organization maintain compliance with privacy regulations?
A. Developing security awareness training
B. Implementing security information and event management (SIEM)
C. Implementing a data classification framework
D. Installing a data loss prevention (DLP) solution
Answer: (SHOW ANSWER)
A data classification framework (C) is the foundational step for privacy compliance because organizations must first understand what data they have, its sensitivity, and how it is regulated. Privacy obligations vary by data type (e.g., personal, sensitive, regulated), and classification enables appropriate handling, protection, retention, and access controls. Awareness training (A), SIEM (B), and DLP (D) are all valuable controls, but they are ineffective or misaligned without knowing which data requires protection and at what level. CISM governance guidance emphasizes that compliance and control selection must be risk- and data-driven, making classification an essential prerequisite for privacy programs.
References: ISACA CISM Review Manual (Governance-data governance, privacy, information asset classification); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 279

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: (SHOW ANSWER)
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: 280
When establishing an information security governance framework, it is MOST important for an information security manager to understand:
Freecram.net
A. risk management techniques.
B. information security best practices.
C. the threat environment.
D. the corporate culture.
Answer: (SHOW ANSWER)

NEW QUESTION: 281
Which of the following tools provides an incident response team with the GREATEST insight into insider threat activity across multiple systems?
A. A security information and event management (SIEM) system
B. An intrusion prevention system (IPS)
C. A virtual private network (VPN) with multi-factor authentication (MFA)
D. An identity and access management (IAM) system
Answer: (SHOW ANSWER)
A SIEM system is the best tool for providing an incident response team with the greatest insight into insider threat activity across multiple systems because it can collect, correlate, analyze, and report on security events and logs from various sources, such as network devices, servers, applications, and user activities. A SIEM system can also detect and alert on anomalous or suspicious behaviors, such as unauthorized access, data exfiltration, privilege escalation, or

policy violations, that may indicate an insider threat. A SIEM system can also support forensic investigations and incident response actions by providing a centralized and comprehensive view of the security posture and incidents.
References: The CISM Review Manual 2023 defines SIEM as "a technology that provides real-time analysis of security alerts generated by network hardware and applications" and states that "SIEM systems can help identify insider threats by correlating user activity logs with other security events and detecting deviations from normal patterns" (p. 184). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A security information and event management (SIEM) system is the correct answer because it can provide the most insight into insider threat activity across multiple systems by collecting, correlating, analyzing, and reporting on security events and logs from various sources" (p. 95). Additionally, the Detecting and Identifying Insider Threats article from the CISA website states that
"threat detection and identification is the process by which persons who might present an insider threat risk due to their observable, concerning behaviors come to the attention of an organization or insider threat team.
Detecting and identifying potential insider threats requires both human and technological elements" and that
"technological elements include tools such as security information and event management (SIEM) systems, user and entity behavior analytics (UEBA) systems, and data loss prevention (DLP) systems, which can monitor, analyze, and alert on user activities and network events" (p. 1)1.

NEW QUESTION: 282
The MAIN benefit of implementing a data loss prevention (DLP) solution is to:
A. enhance the organization's antivirus controls.
B. eliminate the risk of data loss.
C. complement the organization's detective controls.
D. reduce the need for a security awareness program.
Answer: (SHOW ANSWER)
A data loss prevention (DLP) solution is a type of detective control that monitors and prevents unauthorized transmission or leakage of sensitive data from the organization. A DLP solution can enhance the organization' s antivirus controls by detecting and blocking malicious code that attempts to exfiltrate data, but this is not its main benefit. A DLP solution cannot eliminate the risk of data loss, as there may be other sources of data loss that are not covered by the DLP solution, such as physical theft, accidental deletion, or natural disasters. A DLP solution also does not reduce the need for a security awareness program, as human factors are often the root cause of data loss incidents. A security awareness program can educate and motivate employees to follow security policies and best practices, and to report any suspicious or anomalous activities.
References = ISACA, CISM Review Manual, 16th Edition, 2020, page 79.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1003.

NEW QUESTION: 283
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: 284
Which of the following is the BEST indication of an effective information security program?
A. Risk is treated to an acceptable level.
B. The number of security incidents reported by staff has increased.
C. Key risk indicators (KRIs) are established.
D. Policies are reviewed and approved by senior management.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
An effective information security program aims to manage risks to acceptable levels while supporting business objectives.
* A. Risk is treated to an acceptable level: This is the BEST answer as it directly reflects the program's success in mitigating risks within the organization's tolerance levels.
* B. The number of security incidents reported by staff has increased: An increase in reported incidents might indicate improved awareness but does not necessarily reflect overall effectiveness.
* C. Key risk indicators (KRIs) are established: KRIs are important for monitoring risks but do not indicate whether risks are being effectively managed.
* D. Policies are reviewed and approved by senior management: While essential, this action alone does not demonstrate the program's effectiveness.

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

NEW QUESTION: 285
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: 286
While classifying information assets an information security manager notices that several production databases do not have owners assigned to them What is the BEST way to address this situation?
A. Assign responsibility to the database administrator (DBA).
B. Review the databases for sensitive content.

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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 287
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: 288
The PRIMARY goal of a post-incident review should be to
A. determine why the incident occurred
B. identify policy changes to prevent a recurrence
C. determine how to improve the incident handling process
D. establish the cost of the incident to the business.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 289
Which of the following BEST informs the design of an information security framework?
A. Recent audit findings
B. Implementation cost
C. Risk appetite
D. Available skills
Answer: (SHOW ANSWER)
Risk appetite (C) best informs the design of an information security framework because it defines the level of risk the organization is willing to accept in pursuit of its objectives. CISM stresses that security frameworks, policies, and control structures must be aligned with business risk tolerance to avoid over- or under- protection. Audit findings (A) highlight gaps, cost (B) affects feasibility, and available skills (D) influence implementation-but none define the strategic level of protection required. Risk appetite ensures that the framework supports business goals, prioritizes resources appropriately, and provides consistent guidance for decision-making across the organization. References: ISACA CISM Review Manual (Governance-risk appetite, framework design); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 290
Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?
Freecram.net
A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure
Answer: (SHOW ANSWER)
Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security

initiatives. The other choices may also be included in a security report, but security metrics are the most important.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.
The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

NEW QUESTION: 291
Which of the following is the MOST likely reason for a vulnerability scanner to return incomplete results?
A. Zero-day vulnerability signatures have not been ingested.
B. Scan results are not ingested into a security information and event management (SIEM) tool.
C. Unauthenticated vulnerability scans are being performed.
D. Host names have not been fully enumerated.
Answer: (SHOW ANSWER)

NEW QUESTION: 292
An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?
A. Set up communication channels for the target audience.
B. Determine the needs and requirements of each audience.
C. Create a comprehensive singular communication
D. Invoke the organization's incident response plan.
Answer: (SHOW ANSWER)
The information security manager should do FIRST invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a

comprehensive singular communication are all important steps for communicating effectively with the board, regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the relevant information to the target audience according to the plan. References = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012
Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

NEW QUESTION: 293
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: 294
Which of the following BEST indicates that information security governance and corporate governance are integrated?
A. The information security team is aware of business goals.

B. The board is regularly informed of information security key performance indicators (KPIs),
C. The information security steering committee is composed of business leaders.
D. A cost-benefit analysis is conducted on all information security initiatives.
Answer: (SHOW ANSWER)
The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

NEW QUESTION: 295
An organization provides notebook PCs, cable wire locks, smartphone access, and virtual private network (VPN) access to its remote employees. Which of the following is MOST important for the information security manager to ensure?
A. Employees use smartphone tethering when accessing from remote locations.
B. Employees physically lock PCs when leaving the immediate area.
C. Employees are trained on the acceptable use policy.
D. Employees use the VPN when accessing the organization's online resources.
Answer: D (LEAVE A REPLY)
Using the VPN when accessing the organization's online resources is the most important thing to ensure, as it provides a secure and encrypted connection between the remote employees and the organization's network, and protects the data and systems from unauthorized access, interception, or tampering. VPNs also help to comply with the organization's security policies and standards, and to prevent data leakage or breaches.
References = CISM Review Manual 2022, page 3081; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.92; CISM 2020: Remote Access Security; How to Secure Remote Workers with VPN

NEW QUESTION: 296

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: 297

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: 298

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.

NEW QUESTION: 299
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: 300

Which of the following is the BEST way to obtain organization-wide support for an information security program?

Freecram.net

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: 301
Which of the following would BEST address the risk of a system failing to detect a breach?
A. User access reviews
B. Log monitoring
C. Vulnerability scanning
D. Security control testing
Answer: (SHOW ANSWER)
Log monitoring (B) directly addresses the risk of a system failing to detect a breach by enabling continuous visibility into system activity, anomalies, and indicators of compromise. CISM emphasizes detection as a critical component of incident management, with log review and monitoring serving as primary detective controls. User access reviews (A) are preventive and periodic, not real-time. Vulnerability scanning (C) identifies weaknesses but does not detect active breaches. Security control testing (D) validates control design and effectiveness but does not provide ongoing breach detection. Effective log monitoring reduces mean time to detect incidents and limits business impact.
References: ISACA CISM Review Manual (Incident management-detection and monitoring); CISM Exam Content Outline (Domain 4).

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 302
An organization's quality process can BEST support security management by providing:
A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.
Answer: (SHOW ANSWER)
= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct security defects, measure security performance and effectiveness, and improve security practices

and procedures. References = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

NEW QUESTION: 303
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: (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: 304
Which of the following should be done FIRST to prioritize response to incidents?
A. Containment
B. Escalation
C. Analysis
D. Triage
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?
A. Integrity
B. Authenticity
C. Confidentiality
D. Nonrepudiation

Answer: (SHOW ANSWER)
Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References: https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

NEW QUESTION: 306
Which of the following is the MOST important security consideration when planning to use a cloud service provider in a different country?
A. Ability to logically separate client data
B. Ability to meet service level agreements (SLAs)
C. Ability to meet business resiliency requirements
D. Ability to enforce contractual obligations
Answer: (SHOW ANSWER)
When dealing with a provider in another country, the most important consideration is the ability to enforce contractual obligations (D). CISM highlights jurisdictional risk, including differences in laws, regulations, and legal enforcement mechanisms. Logical separation (A), SLAs (B), and resiliency (C) are important but depend on enforceable contracts to be meaningful. Without enforceability, the organization may lack effective recourse in the event of security failures or breaches.
References: ISACA CISM Review Manual (Governance-legal, regulatory, and third-party risk); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 307
Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?
A. Create a security exception.
B. Perform a gap analysis to determine needed resources.
C. Perform a vulnerability assessment.
D. Assess the risk to business operations.
Answer: (SHOW ANSWER)
The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.

References = CISM Review Manual, 16th Edition, page 48

NEW QUESTION: 308
A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:
A. developing a security program that meets global and regional requirements.
B. ensuring effective communication with local regulatory bodies.
C. using industry best practice to meet local legal regulatory requirements.
D. monitoring compliance with defined security policies and standards.
Answer: (SHOW ANSWER)
= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. References = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.
In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

NEW QUESTION: 309
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: 310

Which is following should be an information security manager's PRIMARY focus during the development of a critical system storing highly confidential data?

Freecram.net

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

NEW QUESTION: 311
Which of the following is the BEST strategy when determining an organization's approach to risk treatment?
A. Implementing risk mitigation controls that are considered quick wins
B. Prioritizing controls that directly mitigate the organization's most critical risks
C. Advancing the maturity of existing controls based on risk tolerance

D. Implementing a one-size-fits-all set of controls across all organizational units

Answer: (SHOW ANSWER)

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

"Risk treatment efforts should focus on the most significant risks first, based on likelihood and impact."

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

NEW QUESTION: 312

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: 313

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: 314
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: 315
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. Identify the data to be hosted.
B. Perform a risk assessment.
C. Perform a gap analysis.
D. Analyze the business requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 316
Which of the following should be of GREATEST concern to an information security manager when evaluating a cloud service provider?
A. Data retention policies are not documented

B. There is no right to audit the security of the provider
C. The provider is new to the market and lacks references
D. Security controls offered by the provider are inadequate
Answer: (SHOW ANSWER)
The lack of audit rights prevents the organization from verifying the security posture and compliance of the provider, representing a major governance and assurance gap.
"Right to audit clauses ensure that organizations retain oversight and can verify the security controls and compliance of their service providers."
- CISM Review Manual 15th Edition, Chapter 3: Outsourced Services, Section: Third-Party Governance* Control inadequacy can be fixed; lack of oversight cannot be tolerated.

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 317
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/.

NEW QUESTION: 318
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: 319
The PRIMARY objective of timely declaration of a disaster is to:
A. ensure engagement of business management in the recovery process.
B. assess and correct disaster recovery process deficiencies.
C. protect critical physical assets from further loss.
D. ensure the continuity of the organization's essential services.
Answer: (SHOW ANSWER)
The primary objective of timely declaration of a disaster is to ensure the continuity of the organization's essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan (DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.

References = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

NEW QUESTION: 320

Which of the following should be the PRIMARY objective when establishing a new information security program?

Freecram.net

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: 321

Which of the following is an information security manager's BEST course of action when a penetration test reveals a security exposure due to a firewall that is not configured correctly?

A. Ensure a plan with milestones is developed.

B. Implement a distributed denial of service (DDoS) control.

C. Engage the incident response team.

D. Define new key performance indicators (KPIs).

Answer: (SHOW ANSWER)

A penetration test is a proactive way to identify and remediate security vulnerabilities in a network. When a penetration test reveals a security exposure due to a firewall that is not configured correctly, the information security manager's best course of action is to ensure a plan with milestones is developed to address the issue.

This plan should include the root cause analysis, the corrective actions, the responsible parties, the deadlines, and the verification methods. This way, the information security manager can ensure that the security exposure is resolved in a timely and effective manner, and that the firewall configuration is aligned with the security policy and the business objectives.

References =

CISM Review Manual (Digital Version), page 193: "The information security manager should ensure that a plan with milestones is developed to address the issues identified during the penetration test." How to configure a network firewall: Walkthrough: "A good network firewall is

essential. Learn the basics of configuring a network firewall, including stateful vs. stateless firewalls and access control lists in this episode of Cyber Work Applied." Which of the following is the BEST way to evaluate whether the information security program aligns with corporate governance?
A). Survey mid-level management.
B). Analyze industry benchmarks.
C). Conduct a gap analysis.
D). Review internal audit reports.

NEW QUESTION: 322
Which of the following is the PRIMARY reason to use a phased incident recovery approach?
A. To give the response team time to analyze incidents
B. To ensure critical systems are recovered first
C. To gain management buy-in
D. To prioritize remediation steps
Answer: (SHOW ANSWER)

NEW QUESTION: 323
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: 324
The MOST useful technique for maintaining management support for the information security program is:
A. informing management about the security of business operations.
B. implementing a comprehensive security awareness and training program.
C. identifying the risks and consequences of failure to comply with standards.
D. benchmarking the security programs of comparable organizations.
Answer: (SHOW ANSWER)

= According to the CISM Review Manual, one of the key success factors for an information security program is to maintain management support and commitment. This can be achieved by providing regular reports to management on the security status of the organization, the effectiveness of the security controls, and the alignment of the security program with the business objectives and strategy. By informing management about the security of business operations, the information security manager can demonstrate the value and benefits of the security program, and ensure that management is aware of the security risks and issues that need to be addressed. This technique can also help to build trust and confidence between the information security manager and the senior management, and foster a culture of security within the organization1
The other options are not as effective as informing management about the security of business operations.
Implementing a comprehensive security awareness and training program is important, but it is mainly targeted at the end users and staff, not the senior management. Identifying the risks and consequences of failure to comply with standards can help to justify the need for security controls, but it can also create a negative impression of the security program as being too restrictive or punitive. Benchmarking the security programs of comparable organizations can provide some insights and best practices, but it may not reflect the specific needs and context of the organization, and it may not be relevant or applicable to the management's expectations and priorities1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 28-29...

NEW QUESTION: 325
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?
A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products
D. Unreliable delivery of hardware and software resources by a supplier
Answer: (SHOW ANSWER)
= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness.
Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios

may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page
189 1; CISM Practice Quiz 2

NEW QUESTION: 326
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: 327
Which of the following is the BEST indication that an organization has integrated information security governance with corporate governance?
A. Security performance metrics are measured against business objectives.
B. Impact is measured according to business loss when assessing IT risk.
C. Security policies are reviewed whenever business objectives are changed.
D. Service levels for security vendors are defined according to business needs.
Answer: (SHOW ANSWER)
Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives.
Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 328
Which of the following is the BEST method to ensure compliance with password standards?

A. Implementing password-synchronization software
B. Using password-cracking software
C. Automated enforcement of password syntax rules
D. A user-awareness program
Answer: (SHOW ANSWER)
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.
Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for
2020 - Auth0 2: Password synchronization - Wikipedia 3:

NEW QUESTION: 329
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: C (LEAVE A REPLY)
= 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: 330
What will BEST facilitate the success of new security initiatives?
A. Monitor post-implementation security metrics.
B. Update security policies on a regular basis
C. Establish an IT security steering committee.
D. Include business in security decision making.
Answer: (SHOW ANSWER)

NEW QUESTION: 331
Which of the following is the GREATEST threat posed by quantum computing technology for information security?
A. Quantum computers can break several current encryption schemes protecting the confidentiality of data
B. Quantum computers can allow for secure communication that benefits only the few who can afford it
C. Quantum computers can compromise availability through extremely rapid processing of large data sets
D. Quantum computers can simulate complex physical systems beyond traditional computing capabilities
Answer: (SHOW ANSWER)
The greatest threat posed by quantum computing is its potential to break widely used cryptographic algorithms (A), particularly public-key encryption schemes that rely on mathematical problems vulnerable to quantum algorithms. This directly threatens data confidentiality and long-term data protection. The other options describe secondary or non-security impacts. CISM recognizes cryptographic resilience as a core component of risk management and emphasizes the need for organizations to monitor emerging technologies that could invalidate existing controls. Quantum computing's impact on encryption represents a systemic risk to trust, privacy, and secure communications.
References: ISACA CISM Review Manual (Risk management-emerging technologies and cryptographic risk); CISM Exam Content Outline (Domain 1).

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 332
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: 333
Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?
A. Identify business requirements
B. Document disaster recovery procedures
C. Conduct a risk assessment
D. Perform a business impact analysis (BIA)
Answer: (SHOW ANSWER)
The Business Impact Analysis (BIA) is the first step in developing a disaster recovery plan because it identifies critical business processes, dependencies, and acceptable downtime.
"A BIA provides the foundation for disaster recovery planning by identifying business functions and their criticality."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Disaster Recovery Planning* Risk assessments follow the BIA and inform recovery strategies, but the BIA must come first.

NEW QUESTION: 334
What is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

A. To share responsibility for addressing security breaches
B. To gain acceptance of the policy across the organization
C. To decrease the workload of the IT department
D. To reduce the overall cost of policy development
Answer: (SHOW ANSWER)
Involving stakeholders from various business units promotes buy-in, relevance, and adherence. When users feel they've had input in shaping the policy, they're more likely to support and follow it.
Stakeholders also provide insights into business processes that help ensure policies are practical and tailored.
This collaboration enhances organizational alignment and ensures policies do not create unintended operational friction.
"Stakeholder involvement is key to ensuring that policies are practical, aligned with operations, and accepted throughout the organization."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Policy Development and Implementation*

NEW QUESTION: 335
Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?
A. Include the noncompliance in the risk register
B. Report the noncompliance to senior management
C. Implement compensating controls to mitigate the noncompliance
D. Validate the noncompliance
Answer: (SHOW ANSWER)

NEW QUESTION: 336
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: 337
Which of the following MUST be established to maintain an effective information security governance framework?
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: 338
Which of the following BEST determines the data retention strategy and subsequent policy for an organization?
A. Risk appetite
B. Business requirements
C. Business impact analysis (BIA)
D. Supplier requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 339
Which of the following MOST effectively identifies the organization's ability to comply with legal, regulatory, and contractual requirements?
A. Vulnerability scan
B. Control self-assessment (CSA)
C. Gap analysis
D. Risk assessment
Answer: (SHOW ANSWER)

A gap analysis is the most effective method to identify an organization's ability to comply with legal, regulatory, and contractual requirements because it explicitly compares the current state of controls, policies, and practices against required obligations. In CISM governance, compliance is assessed by determining whether mandatory requirements are fully met, partially met, or not met at all-this is the precise purpose of a gap analysis.
Vulnerability scanning (A) focuses on technical weaknesses and does not assess compliance with laws or contracts. A control self-assessment (CSA) (B) evaluates the effectiveness of existing controls but does not systematically compare them against external compliance requirements. A risk assessment (D) evaluates threats, vulnerabilities, and impacts, but its objective is risk prioritization, not compliance determination.
CISM emphasizes that governance requires clear visibility into compliance gaps so management can prioritize remediation, allocate resources, and demonstrate due diligence. Gap analysis provides structured, auditable evidence of compliance posture and directly supports regulatory readiness and contractual assurance.
References:
ISACA CISM Review Manual, Information Security Governance - compliance management and gap analysis ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

NEW QUESTION: 340
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: 341
An information security manager has been notified that two senior executives have the ability to elevate their own privileges in the corporate accounting system, in violation of policy. What is the FIRST step to address this issue?
A. Perform a system access review.
B. Perform a full review of all system transactions over the past 90 days.
C. Immediately suspend the executives' access privileges.
D. Notify the CISO of the security policy violation.
Answer: (SHOW ANSWER)

NEW QUESTION: 342
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: B (LEAVE A REPLY)
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: 343
Which of the following is the BEST course of action when an information security manager identifies that systems are vulnerable to emerging threats?
A. Frequently update systems and monitor the threat landscape.
B. Monitor the network containing the affected systems for malicious traffic.
C. Increase awareness of the threats among employees who work with the systems.
D. Notify senior management and key stakeholders of the threats.
Answer: (SHOW ANSWER)
The best course of action when an information security manager identifies that systems are vulnerable to emerging threats is to frequently update systems and monitor the threat landscape, as this will help to reduce the exposure and impact of the threats, and enable timely detection and response. Updating systems involves applying patches, fixing vulnerabilities, and implementing security controls. Monitoring the threat landscape involves collecting and analyzing threat intelligence, identifying new attack vectors and techniques, and assessing the risk and impact of the threats.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2211; State of Cybersecurity 2023: Navigating Current and Emerging Threats2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

NEW QUESTION: 344
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: 345
An incident response team has established that an application has been breached. Which of the following should be done NEXT?
A. Maintain the affected systems in a forensically acceptable state
B. Conduct a risk assessment on the affected application
C. Inform senior management of the breach.
D. Isolate the impacted systems from the rest of the network
Answer: D (LEAVE A REPLY)
The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems. References:
https://www.crowdstrike.com/cybersecurity-101/incident-response/
https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

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

NEW QUESTION: 346
Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?
A. Conducting periodic vulnerability assessments
B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework
Answer: (SHOW ANSWER)
The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 347
The MOST effective tools for responding to new and advanced attacks are those that detect attacks based on:
A. data packet analysis.
B. behavior analysis.
C. penetration testing.
D. signature analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 348
Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?
A. Increase the frequency of system backups.
B. Review the mitigating security controls.
C. Notify staff members of the threat.
D. Assess the risk to the organization.
Answer: (SHOW ANSWER)
The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness.
The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of

compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. References = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

NEW QUESTION: 349

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: 350

The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization. Which of the following should be done FIRST?

Freecram.net

A. Inform senior management

B. Re-evaluate the risk

C. Implement compensating controls

D. Ask the business owner for the new remediation plan

Answer: (SHOW ANSWER)

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

This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner.
The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

NEW QUESTION: 351
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?
A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.
Answer: (SHOW ANSWER)
The best course of action when the organization receives complaints from users that some of their files have been encrypted and they are receiving demands for money to decrypt the files is to initiate incident response.
This is because the organization is facing a ransomware attack, which is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and loss to the organization's operations, assets, and reputation. Therefore, the organization needs to quickly activate its incident response plan and team, which are designed to handle such security incidents in a coordinated, effective, and efficient manner. The incident response process involves the following steps1:
Preparation: The incident response team prepares the necessary resources, tools, and procedures to respond to the incident. The team also establishes the roles, responsibilities, and communication channels among the team members and other stakeholders.
Identification: The incident response team identifies the scope, source, and severity of the incident. The team also collects and preserves the relevant evidence and logs for further analysis and investigation.

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

NEW QUESTION: 352
Which of the following is an information security manager's BEST recommendation to senior management following a breach at the organization's Software as a Service (SaaS) vendor?
A. Terminate the relationship with the vendor.
B. Update the vendor risk assessment.
C. Renegotiate the vendor contract.
D. Engage legal counsel.
Answer: (SHOW ANSWER)

NEW QUESTION: 353
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?
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: 354
Which of the following BEST indicates misalignment of security policies with business objectives?
A. Lack of adequate funding for the security program
B. A large number of long-term policy exceptions
C. Low completion rate of employee awareness training
D. A large number of user noncompliance incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 355
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: 356
Which of the following is MOST important when designing an information security governance framework?
A. Aligning with industry best practice frameworks
B. Assessing the availability of information security resources
C. Aligning with the information security strategy
D. Assessing the current state of information security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 357
When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

A. best practices.
B. control framework
C. regulatory requirements.
D. cost-benefit analysis,
Answer: (SHOW ANSWER)
Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls12.
CBA involves the following steps12:
Identify the objectives and scope of the analysis
Identify the alternatives and options for achieving the objectives
Identify and quantify the costs and benefits of each alternative
Compare the costs and benefits of each alternative using a common metric or criteria Select the alternative that maximizes the net benefit or minimizes the net cost Perform a sensitivity analysis to test the robustness and validity of the results Document and communicate the results and recommendations CBA is mainly driven by the information security manager's decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization. Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization's objectives, resources, and environment12. References = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

NEW QUESTION: 358
When defining a security baseline, it is MOST important that the baseline:
A. can vary depending on the security classification of systems.
B. is uniform for all assets of the same type.
C. is developed based on stakeholder consensus.
D. aligns to key risk indicators (KRIs).
Answer: (SHOW ANSWER)

A security baseline is a set of minimum security requirements for a system or asset type. The CISM Review Manual states that a baseline should be uniform for all assets of the same type to ensure consistency, enforceability, and ease of monitoring. This standardization supports effective compliance and security operations. While other factors can influence baseline adjustments, uniformity for similar asset types is most critical.
Reference:ISACA CISM Review Manual, 16th Edition, Page 207, "Establishing Security Baselines".

NEW QUESTION: 359
An organization has suffered from a large-scale security event impacting a critical system. Following the decision to restore the system at an alternate location, which plan should be invoked?
A. Communications plan
B. Business continuity plan (BCP)
C. Incident response plan
D. Disaster recovery plan (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 360
Which of the following is the MOST important reason to document information security incidents that are reported across the organization?
Freecram.net
A. Identify unmitigated risk.
B. Prevent incident recurrence.
C. Evaluate the security posture of the organization.
D. Support business investments in security
Answer: (SHOW ANSWER)

NEW QUESTION: 361
Which of the following is the MOST essential element of an information security program?
A. Benchmarking the program with global standards for relevance
B. Prioritizing program deliverables based on available resources
C. Involving functional managers in program development
D. Applying project management practices used by the business
Answer: (SHOW ANSWER)
Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives.
References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units." CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 362
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: 363
The resilience requirements of an application are BEST determined by:
A. A risk assessment

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

NEW QUESTION: 364
Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?
A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.
Answer: (SHOW ANSWER)
The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:
Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of

the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

NEW QUESTION: 365
Which of the following BEST enables an organization to evaluate the security posture of a cloud service?
A. Industry peer reviews
B. Service provider attestations
C. Penetration testing reports
D. Third-party audit reports
Answer: (SHOW ANSWER)
Third-party audit reports (D) provide the most reliable evaluation of a cloud provider's security posture because they offer independent assurance of control design and effectiveness. Peer reviews (A) and attestations (B) are less objective, while penetration test reports (C) focus narrowly on technical vulnerabilities. CISM emphasizes independent assurance mechanisms when assessing third-party security, particularly for cloud services.
References: ISACA CISM Review Manual (Governance-third-party assurance and cloud risk); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 366
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: 367
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: 368
Which of the following is the BEST way to ensure the capability to restore clean data after a ransomware attack?
A. Purchase cyber insurance
B. Encrypt sensitive production data
C. Perform Integrity checks on backups
D. Maintain multiple offline backups
Answer: (SHOW ANSWER)
The best way to ensure the capability to restore clean data after a ransomware attack is to maintain multiple offline backups. Offline backups are backups that are not connected to the network or the internet, and therefore are not accessible by ransomware. Multiple offline backups provide redundancy and allow the organization to choose the most recent and uncorrupted backup to restore the data. Offline backups should be stored in a secure location and tested regularly to ensure their integrity and availability.
Purchasing cyber insurance may help the organization cover some of the costs associated with a ransomware attack, such as ransom payment, data recovery, legal fees, etc., but it does not guarantee the capability to restore clean data. Cyber insurance policies may have exclusions, limitations, or conditions that affect the coverage and reimbursement. Moreover, cyber insurance does not prevent or mitigate the ransomware attack itself, and it may not cover all the losses or damages caused by the attack.
Encrypting sensitive production data may protect the confidentiality of the data from unauthorized access or disclosure, but it does not prevent ransomware from encrypting the data again. Ransomware does not need to decrypt the data to encrypt it, and it may use a different encryption algorithm or key than the one used by the organization. Encrypting production data may also increase the complexity and time required for data recovery, especially if the encryption keys are lost or compromised.
Performing integrity checks on backups may help the organization verify that the backups are not corrupted or tampered with, but it does not ensure the capability to restore clean data after a ransomware attack. Integrity checks are a preventive measure that should be done before the attack, not after. If the backups are already infected or encrypted by ransomware, performing integrity checks will not help to recover the data. Integrity checks should be complemented by other measures, such as isolation, versioning, and offline storage, to protect the backups from ransomware. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3081; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Ransomware recovery: 8 steps to successfully restore from backup3; Ransomware Recovery: 5 Steps to Recover Data4

NEW QUESTION: 369

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

A. Consult with IT staff and assess the risk based on their recommendations

B. Update the security policy based on the regulatory requirements

C. Propose relevant controls to ensure the business complies with the regulation

D. Identify and assess the risk in the context of business objectives

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 370

Which is MOST important to identify when developing an effective information security strategy?

A. Security awareness training needs

B. Potential savings resulting from security governance

C. Business assets to be secured

D. Residual risk levels

Answer: (SHOW ANSWER)

Business assets are the resources that enable the organization to achieve its objectives and create value.

Identifying the business assets to be secured is the most important step in developing an effective information security strategy, as it helps to align the security goals with the business goals, prioritize the security efforts and resources, and define the scope and boundaries of the security program. (From CISM Review Manual
15th Edition)

References: CISM Review Manual 15th Edition, page 27, section 1.2.1.

NEW QUESTION: 371

An organization is about to purchase a rival organization. The PRIMARY reason for performing information security due diligence prior to making the purchase is to:

A. determine the security exposures.

B. assess the ability to integrate the security department operations.

C. ensure compliance with international standards.

D. evaluate the security policy and standards.

Answer: (SHOW ANSWER)

Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value,

reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnair

NEW QUESTION: 372
An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?
A. Create a business case for a new incident response plan.
B. Revise the existing incident response plan.
C. Conduct a gap analysis.
D. Assess the impact to the budget,
Answer: (SHOW ANSWER)
Before implementing any changes to the security incident response plan, the information security manager should first conduct a gap analysis to identify the current state of the plan and compare it with the new requirements. A gap analysis is a systematic process of evaluating the differences between the current and desired state of a system, process, or program. A gap analysis can help to identify the strengths and weaknesses of the existing plan, the gaps that need to be addressed, the priorities and dependencies of the actions, and the resources and costs involved. A gap analysis can also help to create a business case for the changes and justify the investment. A gap analysis can be conducted using various methods and tools, such as frameworks, standards, benchmarks, questionnaires, interviews, audits, or tests1234.
References =
* CISM Review Manual 15th Edition, page 1631
* CISM certified information security manager study guide, page 452
* How To Conduct An Information Security Gap Analysis3
* PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS4

NEW QUESTION: 373
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?
A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process
Answer: (SHOW ANSWER)
A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right

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

NEW QUESTION: 374
Which of the following is the FIRST step when conducting a post-incident review?
A. Identify mitigating controls.
B. Assess the costs of the incident.
C. Perform root cause analysis.
D. Assign responsibility for corrective actions.
Answer: C (LEAVE A REPLY)
A post-incident review is a process of analyzing an incident and its impact, identifying the root causes, and recommending corrective actions to prevent recurrence. The first step of a post-incident review is to perform root cause analysis, which is the process of identifying the underlying factors that contributed to the occurrence and severity of the incident. Root cause analysis helps to determine the most effective and efficient solutions to address the problem and avoid future incidents. References = CISM Review Manual,
16th Edition, Chapter 5, Section 5.5.2.11

NEW QUESTION: 375
A business continuity plan (BCP) should contain:
A. hardware and software inventories.
B. information about eradication activities.
C. criteria for activation.
D. data restoration procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 376
A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What should be done NEXT?

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

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 377
Which of the following would provide the MOST value to senior management when presenting the results of a risk assessment?
A. Illustrating risk on a heat map
B. Providing a technical risk assessment report
C. Mapping the risks to existing controls
D. Mapping the risks to the security classification scheme
Answer: (SHOW ANSWER)

NEW QUESTION: 378
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: D (LEAVE A REPLY)
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: 379
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: A (LEAVE A REPLY)
= 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: 380
Which of the following is the PRIMARY reason to conduct a post-incident review?
A. To improve the response process
B. To notify regulatory authorities
C. To determine whether digital evidence is admissible
D. To aid in future risk assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 381
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: 382
An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?
A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.
Answer: B (LEAVE A REPLY)
The information security manager should present a business case for additional controls to senior management, as this is the most effective way to communicate the risk and the need for mitigation. The information security manager should not instruct IT to deploy controls based on urgent business needs, as this may not align with the business objectives and may cause unnecessary costs and delays. The information security manager should not solicit bids for compensating control products, as this may not address the root cause of the risk and may not be the best solution. The information security manager should not recommend a different application, as this may not be feasible or desirable for the business. References = CISM Review Manual 2023, page 711; CISM Review Questions, Answers & Explanations Manual 2023, page 252

NEW QUESTION: 383
Who is BEST positioned to take ownership of critical IT security risks identified in an application?
A. Chief information officer (CIO)
B. Chief information security officer (CISO)
C. Business application owner
D. Lead application developer
Answer: (SHOW ANSWER)
The business application owner (C) is best positioned to own application-related security risks because they are accountable for the business outcomes, value, and operational impact of the application. CISM consistently assigns risk ownership to business roles, not technical implementers. The CISO (B) advises on security posture, the CIO (A) oversees IT strategy, and developers (D) implement controls-but none are accountable for accepting or prioritizing business risk. Assigning ownership to the application owner ensures that risk decisions reflect business priorities and align with risk appetite.
References: ISACA CISM Review Manual (Governance-risk ownership and accountability); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 384

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

A. Security maturity assessment results

B. Threat analysis of the organization's environment

C. Results of vulnerability assessments

D. External penetration test findings

Answer: (SHOW ANSWER)

A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture.

"Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models* Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

NEW QUESTION: 385

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: 386
What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?
A. Vendor service level agreements (SLAs)
B. Independent review of the vendor
C. Local laws and regulations
D. Backup and restoration of data
Answer: (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: 387
Which of the following is the BEST indicator of a successful intrusion into an organization's systems?
A. Increase in the number of failed login attempts

B. Decrease in available storage space
C. Decrease in internal network traffic
D. Increase in the number of irregular application requests
Answer: D (LEAVE A REPLY)

NEW QUESTION: 388
Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?
A. Conduct a cost-benefit analysis.
B. Consult corporate legal counsel
C. Update the information security policy.
D. Perform a gap analysis.
Answer: (SHOW ANSWER)
When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 389
When determining an acceptable risk level which of the following is the MOST important consideration?
A. Threat profiles
B. System criticalities
C. Vulnerability scores
D. Risk matrices
Answer: (SHOW ANSWER)
The effectiveness of an incident response team will be greatest when the incident response process is updated based on lessons learned. This ensures that the team can continuously improve its performance and capabilities, and address any gaps or weaknesses identified during previous incidents. Updating the incident response process based on lessons learned also helps to align the process with the changing business and security environment, and to incorporate best practices and standards. Meeting on a regular basis to review log files, having trained security personnel as team members, and using a security information and event monitoring (SIEM) system are all important factors for an incident response team, but they are not sufficient to ensure the effectiveness of the team. Reviewing log files may help to detect and analyze incidents, but it does not guarantee that the team can respond appropriately and efficiently.

Having trained security personnel may enhance the skills and knowledge of the team, but it does not ensure that the team can work collaboratively and communicate effectively. Using a SIEM system may facilitate the identification and prioritization of incidents, but it does not ensure that the team can follow the established procedures and protocols. References = CISM Review Manual, 16th Edition, page 1361; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492

NEW QUESTION: 390

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

Freecram.net

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: 391
Network sniffing is difficult to detect because it can be performed:
A. Passively.
B. Continuously.
C. Actively.
D. Remotely.
Answer: A (LEAVE A REPLY)
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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 392
Which of the following is MOST appropriate to communicate to senior management regarding information risk?
A. Emerging security technologies
B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress
Answer: (SHOW ANSWER)
Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2:
Information Risk Management (IRM) [2022 update]

NEW QUESTION: 393
Of the following, who is BEST suited to own the risk discovered in an application?
A. Senior management
B. Information security manager
C. Control owner
D. System owner

Answer: (SHOW ANSWER)

NEW QUESTION: 394
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: 395
How does an incident response team BEST leverage the results of a business impact analysis (BIA)?
A. Assigning restoration priority during incidents
B. Determining total cost of ownership (TCO)
C. Evaluating vendors critical to business recovery
D. Calculating residual risk after the incident recovery phase
Answer: (SHOW ANSWER)
The incident response team can best leverage the results of a business impact analysis (BIA) by assigning restoration priority during incidents. A BIA is a process that identifies and evaluates the criticality and dependency of the organization's business functions, processes, and resources, and the potential impacts and consequences of their disruption or loss. The BIA results provide the basis for determining the recovery objectives, strategies, and plans for the organization's

business continuity and disaster recovery. By using the BIA results, the incident response team can prioritize the restoration of the most critical and time-sensitive business functions, processes, and resources, and allocate the appropriate resources, personnel, and time to minimize the impact and duration of the incident.
Determining total cost of ownership (TCO) (B) is not a relevant way to leverage the results of a BIA, as it is not directly related to incident response. TCO is a financial metric that estimates the total direct and indirect costs of owning and operating an asset or a system over its lifecycle. TCO may be useful for evaluating the cost-effectiveness and return on investment of different security solutions or alternatives, but it does not help the incident response team to respond to or recover from an incident.
Evaluating vendors critical to business recovery is also not a relevant way to leverage the results of a BIA, as it is not a primary responsibility of the incident response team. Evaluating vendors critical to business recovery is a part of the vendor management process, which involves selecting, contracting, monitoring, and reviewing the vendors that provide essential products or services to support the organization's business continuity and disaster recovery. Evaluating vendors critical to business recovery may be done before or after an incident, but not during an incident, as it does not contribute to the incident response or restoration activities.
Calculating residual risk after the incident recovery phase (D) is also not a relevant way to leverage the results of a BIA, as it is not a timely or effective use of the BIA results. Residual risk is the risk that remains after the implementation of risk treatment or mitigation measures. Calculating residual risk after the incident recovery phase may be done as a part of the incident review or improvement process, but not during the incident response or restoration phase, as it does not help the incident response team to resolve or contain the incident.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Business Impact Analysis, page 182-1831

NEW QUESTION: 396
An organization recently updated and published its information security policy and standards. What should the information security manager do NEXT?
A. Conduct a risk assessment.
B. Communicate the changes to stakeholders.
C. Update the organization's risk register.
D. Develop a policy exception process.
Answer: (SHOW ANSWER)
Communicating the changes to stakeholders is the next step after updating and publishing the information security policy and standards, as it ensures that the stakeholders are aware of the new or revised requirements, expectations and responsibilities, and can provide feedback or raise concerns if needed. Communication also helps to promote the acceptance and adoption of the policy and standards, and to reinforce the security culture and awareness within the organization.

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

NEW QUESTION: 397
Which of the following is the BEST approach to incident response for an organization migrating to a cloud- based solution?
A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.
Answer: (SHOW ANSWER)
The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles and responsibilities, service level agreements, notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.
The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment.
References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-
192, 195-196, 199-200.
Cloud Incident Response Framework - A Quick Guide 2, pages 3-4, 6-7, 9-10.
CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

NEW QUESTION: 398
Which of the following is MOST important for the effective implementation of an information security governance program?
A. Employees receive customized information security training
B. The program budget is approved and monitored by senior management
C. The program goals are communicated and understood by the organization.

D. Information security roles and responsibilities are documented.

Answer: (SHOW ANSWER)

The program goals are communicated and understood by the organization is the most important factor for the effective implementation of an information security governance program because it ensures that the program is aligned with the business objectives and supported by the stakeholders. Employees receive customized information security training is not the most important factor, but rather a means to achieve the program goals and raise awareness among the staff. The program budget is approved and monitored by senior management is not the most important factor, but rather a resource to enable the program activities and measure its performance. Information security roles and responsibilities are documented is not the most important factor, but rather a way to define and assign the program tasks and accountabilities.

References: https://www.isaca.
org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-information-security- governance https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

NEW QUESTION: 399

Which of the following roles is accountable for the protection of data?

A. CISO

B. Data custodian

C. Data owner

D. Data administrator

Answer: (SHOW ANSWER)

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: 400

Which of the following is MOST important to have in place for an organization's information security program to be effective?

Freecram.net

A. Documented information security processes

B. A comprehensive IT strategy

C. Senior management support

D. Defined and allocated budget

Answer: C (LEAVE A REPLY)
Senior management support is the most important factor to have in place for an organization's information security program to be effective because it helps to establish the vision, direction, and goals of the program, as well as to allocate the necessary resources and authority to implement and maintain it. Senior management support also helps to foster a security culture within the organization, where security is seen as a shared responsibility and a business enabler. Senior management support also helps to ensure compliance with internal and external security policies and standards, as well as to communicate the value and impact of security to stakeholders. Therefore, senior management support is the correct answer.
References:
* https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for- security-governance-part-1
* https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf
* https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d

NEW QUESTION: 401
A balanced scorecard MOST effectively enables information security:
A. risk management
B. project management
C. governance
D. performance
Answer: (SHOW ANSWER)
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: 402
Which of the following should an information security manager do FIRST upon learning that a competitor has experienced a ransomware attack?
A. Review the current risk assessment.
B. Update indicators of compromise in the security systems.
C. Conduct ransomware awareness training for all staff.
D. Perform a full data backup.
Answer: (SHOW ANSWER)

NEW QUESTION: 403

When testing an incident response plan for recovery from a ransomware attack, which of the following is MOST important to verify?

A. Digital currency is immediately available.

B. Network access requires two-factor authentication.

C. Data backups are recoverable from an offsite location.

D. An alternative network link is immediately available.

Answer: (SHOW ANSWER)

Data backups are recoverable from an offsite location is the most important thing to verify when testing an incident response plan for recovery from a ransomware attack, as it ensures that the organization can restore its data and resume its operations without paying the ransom or losing critical information. Data backups should be performed regularly, stored securely, and tested for integrity and availability. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 404

The executive management of a domestic organization has announced plans to expand operations to multiple international locations. Which of the following should be the information security manager's FIRST step upon learning of these plans?

A. Perform a gap analysis against international information security standards

B. Update security training and awareness resources accordingly

C. Research legal and regulatory requirements impacting the new locations

D. Prepare localized information security policies for each new location

Answer: (SHOW ANSWER)

The first step is to research legal and regulatory requirements for the new locations. Different countries have varying security and privacy laws, and understanding these is critical before adapting policies or procedures.

"Security requirements will vary depending on local legal and regulatory obligations, which must be understood as part of international expansion."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Requirements The ISACA CISM practice database also highlights this step as the initial and critical move in international expansions.

NEW QUESTION: 405

An organization's automated security monitoring tool generates an excessively large amount of falsq positives. Which of the following is the BEST method to optimize the monitoring process?

A. Report only critical alerts.

B. Change reporting thresholds.

C. Reconfigure log recording.

D. Monitor incidents in a specific time frame.

Answer: B (LEAVE A REPLY)

Changing reporting thresholds is the best method to optimize the monitoring process when the automated security monitoring tool generates an excessively large amount of false positives. Changing reporting thresholds means adjusting the criteria or parameters that trigger the alerts, such as the severity level, the frequency, the source, or the destination of the events. Changing reporting thresholds can help to reduce the number of false positives, filter out the irrelevant or benign events, and focus on the most critical and suspicious events that require further investigation or response.
References = Cybersecurity tool sprawl leading to burnout, false positives: report, Security tools' effectiveness hampered by false positives

NEW QUESTION: 406
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?
A. Configuration management
B. Risk management
C. Access control management
D. Change management
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the organization's business strategy and objectives, as well as complying with applicable laws and regulations1.
The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.
The CISM Exam Content Outline also covers the topic of change management in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:
3.2.2 Change Management
3.2.3 Change Control
3.2.4 Change Implementation
3.2.5 Change Monitoring
I hope this answer helps you prepare for your CISM exam. Good luck!

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 407
A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated FIRST?
A. Local regulatory requirements
B. Global framework standards
C. Training requirements of the framework
D. Cross-border data mobility
Answer: (SHOW ANSWER)

NEW QUESTION: 408
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: 409
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: 410
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: 411
Which of the following BEST enables the assignment of risk and control ownership?
A. Aligning to an industry-recognized control framework
B. Adopting a risk management framework
C. Obtaining senior management buy-in
D. Developing an information security strategy
Answer: (SHOW ANSWER)
Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.

References:
* https://www.protechtgroup.com/en-au/blog/risk-control-management
* https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_risk_ownership_right.ashx
* https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

NEW QUESTION: 412
Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?
A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider
Answer: (SHOW ANSWER)
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider. References:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a- long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117- p599mr

NEW QUESTION: 413
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: 414
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: (SHOW ANSWER)
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: 415
Which of the following is the MOST important outcome of effective risk treatment?
A. Elimination of risk
B. Timely reporting of incidents
C. Reduced cost of acquiring controls
D. Implementation of corrective actions
Answer: (SHOW ANSWER)
The most important outcome of effective risk treatment is the implementation of corrective actions that address the root causes of the risk and reduce its likelihood and/or impact to an acceptable level. Effective risk treatment does not necessarily eliminate the risk, but rather brings it within the organization's risk appetite and tolerance. Timely reporting of incidents and reduced cost of acquiring controls are desirable benefits of effective risk treatment, but they are not the primary outcome.
References: The CISM Review Manual 2023 defines risk treatment as "the process of selecting and implementing measures to modify risk" and states that "the objective of risk treatment is to implement corrective actions that will reduce the risk to a level that is acceptable to the enterprise" (p. 92). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Implementation of corrective actions is the correct answer because it is the most important outcome of effective risk treatment, as it ensures that the risk is managed in accordance with the organization's risk appetite and tolerance" (p. 28). Additionally, the Not All Risk Treatment Options Are the Same article from the ISACA Journal 2021 states that "risk treatment is the process of implementing corrective actions to address the root causes of the risk and to reduce the likelihood and/or impact of the risk" (p. 1)1.

NEW QUESTION: 416
Spoofing should be prevented because it may be used to:
A. gain illegal entry to a secure system by faking the sender's address,
B. predict which way a program will branch when an option is presented
C. assemble information, track traffic, and identify network vulnerabilities.
D. capture information such as passwords traveling through the network
Answer: (SHOW ANSWER)
Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or

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

NEW QUESTION: 417
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: A (LEAVE A REPLY)
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: 418
A Seat a-hosting organization's data center houses servers, appli
BEST approach for developing a physical access control policy for the organization?
A. Review customers' security policies.
B. Conduct a risk assessment to determine security risks and mitigating controls.
C. Develop access control requirements for each system and application.

D. Design single sign-on (SSO) or federated access.

Answer: (SHOW ANSWER)

= The best approach for developing a physical access control policy for the organization is to conduct a risk assessment to determine the security risks and mitigating controls that are relevant and appropriate for the organization's data center. A risk assessment is a process of identifying, analyzing, and evaluating the information security risks that could affect the availability, integrity, or confidentiality of the servers, applications, and data that are hosted in the data center. A risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate physical access to the data center, such as theft, damage, sabotage, or espionage, and the potential consequences for the organization and its customers, such as service disruption, data loss, data breach, or legal liability. A risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to prevent, detect, or respond to the physical access incidents, such as locks, alarms, cameras, guards, badges, or logs. A risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the physical access control policy and the risk management process.

Reviewing customers' security policies, developing access control requirements for each system and application, and designing single sign-on (SSO) or federated access are all possible steps that the organization can take after conducting the risk assessment, but they are not the best ones. Reviewing customers' security policies is a process of understanding and complying with the customers' expectations and requirements for the security of their servers, applications, and data that are hosted in the data center, and ensuring that the organization's physical access control policy is consistent and compatible with them. Developing access control requirements for each system and application is a process of defining and implementing the specific rules and criteria for granting or denying the physical access to the servers and applications that are hosted in the data center, based on the roles, responsibilities, and privileges of the users, and the sensitivity and criticality of the systems and applications. Designing single sign-on (SSO) or federated access is a process of enabling and facilitating the authentication and authorization of the users who need to access the servers and applications that are hosted in the data center, by using a single or shared identity and credential across multiple systems and domains. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1542

NEW QUESTION: 419

Which of the following should an information security manager do FIRST after identifying suspicious activity on a PC that is not in the organization's IT asset inventory?

A. Isolate the PC from the network

B. Perform a vulnerability scan

C. Determine why the PC is not included in the inventory

D. Reinforce information security training

Answer: (SHOW ANSWER)

The first thing an information security manager should do after identifying suspicious activity on a PC that is not in the organization's IT asset inventory is to determine why the PC is not included in the inventory. This will help to identify the source and scope of the threat, as well as the potential impact and risk to the organization. The IT asset inventory is a list of all the hardware, software, data, and other resources that are owned, controlled, or used by an organization. It helps to establish accountability, visibility, and control over the IT assets, as well as to support security policies and procedures.

If a PC is not included in the inventory, it may indicate that it has been compromised by an unauthorized user or entity, or that it has been moved or transferred without proper authorization. It may also indicate that there are gaps or errors in the inventory management process, such as missing records, duplicate entries, outdated information, or inaccurate classification. These issues can pose significant challenges for information security management, such as:

* Lack of visibility into the IT environment and assets
* Difficulty in detecting and responding to incidents
* Increased risk of data breaches and cyberattacks
* Non-compliance with regulatory requirements and standards
* Reduced trust and confidence among stakeholders

Therefore, an information security manager should take immediate steps to investigate why the PC is not included in the inventory and take appropriate actions to remediate the situation.

References = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Inventory Management1

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

NEW QUESTION: 420

Freecram.net

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: 421
An investigation of a recent security incident determined that the root cause was negligent handing of incident alerts by system admit manager to address this issue?
A. Conduct a risk assessment and share the result with senior management.
B. Revise the incident response plan-to align with business processes.
C. Provide incident response training to data custodians.
D. Provide incident response training to data owners.
Answer: (SHOW ANSWER)
The best action for the system admin manager to address the issue of negligent handling of incident alerts by system admins is to provide incident response training to data custodians because it helps to improve their awareness and skills in recognizing and reporting security incidents, and following the incident response procedures and protocols. Conducting a risk assessment and sharing the result with senior management is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Revising the incident response plan to align with business processes is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Providing incident response training to data owners is not a good action because data owners are not responsible for handling incident alerts or performing incident response tasks. 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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 422
For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:
A. consistent security.
B. comprehensive audits
C. a security-aware culture
D. compliance with policy
Answer: (SHOW ANSWER)
Consistent security is the primary reason for integrating the various assurance functions of an organization for the information security manager because it ensures that the security policies and standards are applied uniformly and effectively across different domains, processes, and systems of the organization.
Comprehensive audits are not the primary reason for integrating the various assurance functions, but rather a possible outcome or benefit of doing so. A security-aware culture is not the primary reason for integrating the various assurance functions, but rather a desirable state or goal of the organization. Compliance with policy is not the primary reason for integrating the various assurance functions, but rather a basic requirement or expectation of the organization.
References: https://www.isaca.org/resources/isaca-journal/issues/2016 /volume-4/integrating-assurance-functions https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

NEW QUESTION: 423
Which of the following is MOST important to include in an information security status report to senior management?
A. Key risk indicators (KRIs)
B. Review of information security policies
C. Information security budget requests
D. List of recent security events
Answer: (SHOW ANSWER)
According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

NEW QUESTION: 424

Which of the following should be of GREATEST concern regarding an organization's security controls?

A. Some controls are performing outside of an acceptable range.

B. No key control indicators (KCIs) have been implemented.

C. Control ownership has not been updated.

D. Control gap analysis is outdated.

Answer: B (LEAVE A REPLY)

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

The organization cannot assess if controls are working as intended

It's difficult to demonstrate due diligence

Risks may go unnoticed

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

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

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

NEW QUESTION: 425

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

A. Consult the record retention policy.

B. Update the awareness and training program.

C. Implement media sanitization procedures.

D. Consult the backup and recovery policy.

Answer: A (LEAVE A REPLY)

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

References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after

identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

NEW QUESTION: 426
A security incident has been reported within an organization. When should an information security manager contact the information owner?
A. After the incident has been contained
B. After the incident has been mitigated
C. After the incident has been confirmed
D. After the potential incident has been logged
Answer: (SHOW ANSWER)
The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 427
A new information security manager finds that the organization tends to use short-term solutions to address problems. Resource allocation and spending are not effectively tracked, and there is no assurance that compliance requirements are being met. What should be done FIRST to reverse this bottom-up approach to security?
A. Establish an audit committee.
B. Create an information security steering committee.
C. Conduct a threat analysis.
D. Implement an information security awareness training program.
Answer: (SHOW ANSWER)

NEW QUESTION: 428
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: 429
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?
A. Applying global security standards to the IT projects
B. Training project managers on risk assessment
C. Integrating the risk assessment into the internal audit program
D. Having the information security manager participate on the project steering committees
Answer: D (LEAVE A REPLY)

NEW QUESTION: 430
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?
Freecram.net
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: 431
When analyzing the emerging risk and threat landscape, an information security manager should FIRST:
A. determine the impact if threats materialize.
B. determine the sources of emerging threats.
C. map threats to business assets.
D. review historical threats within the industry.
Answer: (SHOW ANSWER)

NEW QUESTION: 432
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: 433
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: 434

Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?

A. Information security incidents

B. Availability of potential resources

C. Current resourcing levels

D. Information security strategy

Answer: (SHOW ANSWER)

NEW QUESTION: 435

Which of the following should be the PRIMARY focus of a lessons learned exercise following a successful response to a cybersecurity incident?

A. Establishing the root cause of the incident

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

NEW QUESTION: 436
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?
A. Ensuring hashing of administrator credentials
B. Enforcing service level agreements (SLAs)
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process
Answer: (SHOW ANSWER)
Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 437
Which of the following BEST enables an organization to continuously assess the information security risk posture?
A. Key risk indicators (KRIs)
B. Compliance with industry regulations
C. Periodic review of the risk register
D. Degree of senior management support
Answer: A (LEAVE A REPLY)

NEW QUESTION: 438
Which of the following is the BEST source of information to support an organization's information security vision and strategy?
A. Governance policies
B. Enterprise information security architecture
C. Capability maturity model
D. Metrics dashboard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 439
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: 440
Which of the following is the MOST important consideration when defining control objectives?
A. Senior management support
B. Risk appetite
C. Threat environment
D. Budget allocation
Answer: (SHOW ANSWER)
Risk appetite reflects how much risk the organization is willing to tolerate. It is the primary driver when defining control objectives, ensuring alignment with overall business strategy.
"Risk appetite should be used to guide the selection and design of control objectives to ensure risk is managed within acceptable boundaries."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management Strategy* Support, budget, and threats matter, but without alignment to risk appetite, controls may be misaligned.

NEW QUESTION: 441
An organization learns that a third party has outsourced critical functions to another external provider. Which of the following is the information security manager's MOST important course of action?
A. Engage an independent audit of the third party's external provider.
B. Recommend canceling the contract with the third party.
C. Evaluate the third party's agreements with its external provider.
D. Conduct an external audit of the contracted third party.
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the information security manager should evaluate the third party's agreements with its external provider to ensure that the security requirements and controls are adequate and consistent with the organization's expectations. Engaging or

conducting an audit may be a subsequent step, but not the most important one. Recommending canceling the contract may be premature and impractical.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.2, page 1431.

NEW QUESTION: 442
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?
A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.
Answer: (SHOW ANSWER)
The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

NEW QUESTION: 443
Which of the following is the BEST approach when creating a security policy for a global organization subject to varying laws and regulations?
A. Incorporate policy statements derived from third-party standards and benchmarks.
B. Adhere to a unique corporate privacy and security standard
C. Establish baseline standards for all locations and add supplemental standards as required
D. Require that all locations comply with a generally accepted set of industry
Answer: (SHOW ANSWER)
= Creating a security policy for a global organization subject to varying laws and regulations is a challenging task, as it requires balancing the need for consistency, compliance, and flexibility. The best approach is to establish baseline standards for all locations that reflect the organization's overall security objectives, principles, and requirements. These standards should be aligned with the organization's mission, vision, values, and strategy, as well as with the applicable laws and regulations of each location. The baseline standards should also be reviewed and updated periodically to ensure their relevance and effectiveness.
Additionally, supplemental standards can be added as required to address specific issues or risks that may arise in different locations or situations. Supplemental standards should be based on the best practices and lessons learned from the baseline standards, as well as on the feedback and input from the stakeholders of each location. References = CISM Review Manual, 16th Edition, page 1001

NEW QUESTION: 444

Which of the following should be the FIRST consideration when developing a strategy for protecting an organization's data?

A. Access rights

B. Access monitoring

C. Encryption

D. Classification

Answer: (SHOW ANSWER)

NEW QUESTION: 445

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: 446

Which of the following BEST protects against emerging advanced persistent threat (APT) actors?

A. Honeypot environment
B. Updated security awareness materials
C. Ongoing incident response training
D. Proactive monitoring
Answer: (SHOW ANSWER)
Proactive monitoring (e.g., threat hunting, real-time log analysis, anomaly detection) is the most effective defense against Advanced Persistent Threats (APTs), which are stealthy, well-resourced, and long-term attacks.
APT actors:
Use zero-day exploits
Maintain long-term unauthorized access
Avoid detection
Traditional controls often fail. Proactive monitoring detects anomalies early, allowing for faster mitigation.
"Ongoing monitoring and detection programs are essential for identifying and responding to persistent and evolving threats."
- CISM Review Manual 15th Edition, Chapter 4: Threat Management, Section: APT Detection Techniques*

NEW QUESTION: 447
Which of the following is MOST important for an information security manager to consider when reviewing a security investment plan?
A. The plan resolves all potential threats to business processes.
B. The plan is based on a review of threats and vulnerabilities.
C. The plan focuses on meeting industry best practices and industry standards.
D. The plan has summarized IT costs for implementation.
Answer: (SHOW ANSWER)

NEW QUESTION: 448
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: A (LEAVE A REPLY)
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: 449
Which of the following roles is PRIMARILY responsible for developing an information classification framework based on business needs?
A. Information security manager
B. Information security steering committee
C. Information owner
D. Senior management
Answer: C (LEAVE A REPLY)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, Information owners are responsible for developing an information classification framework based on business needs1. They are also responsible for defining and maintaining the classification scheme, policies, and procedures for their information assets1.
The CISM Review Manual (Digital Version) also states that information owners should collaborate with other stakeholders, such as information security managers, information security steering committees, senior management, and legal counsel, to ensure that the classification framework is aligned with the organization's objectives and complies with applicable laws and regulations1.
The CISM Exam Content Outline also covers the topic of information classification frameworks in Domain 3
- Information Security Program Development and Management (27% exam weight)2. The subtopics include:
* 3.2.1 Information Classification Frameworks
* 3.2.2 Information Classification Policies
* 3.2.3 Information Classification Procedures
* 3.2.4 Information Classification Training
I hope this answer helps you prepare for your CISM exam. Good luck! #

NEW QUESTION: 450
An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?
Freecram.net
A. Initiate incident response.
B. Disable remote
C. Initiate a device reset.
D. Conduct a risk assessment.

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

NEW QUESTION: 451
Which of the following would MOST effectively ensure that a new server is appropriately secured?
A. Performing secure code reviews
B. Enforcing technical security standards
C. Conducting penetration testing
D. Initiating security scanning
Answer: (SHOW ANSWER)
Enforcing technical security standards is the most effective way to ensure that a new server is appropriately secured because it ensures that the server complies with the organization's security policies and best practices, such as encryption, authentication, patching, and hardening.
Performing secure code reviews is not relevant for securing a new server, unless it is running custom applications that need to be verified for security flaws.
Conducting penetration testing is not sufficient for securing a new server, because it only identifies vulnerabilities that can be exploited by attackers, but does not fix them. Initiating security scanning is not sufficient for securing a new server, because it only detects known vulnerabilities or misconfigurations, but does not enforce security standards or remediate issues.
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-3/secure-code-review https://www.isaca.org/resources/isaca- journal/issues/2017/volume-2/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal /issues/2016/volume-5/security-scanning-versus-penetration-testing

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 452
Which of the following should be the PRIMARY basis for determining the value of assets?
A. Cost of replacing the assets
B. Business cost when assets are not available
C. Original cost of the assets minus depreciation
D. Total cost of ownership (TCO)
Answer: (SHOW ANSWER)
The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. References = CISM Review Manual 15th Edition, page 64, page 65.

NEW QUESTION: 453
Which of the following is the BEST way to reduce the risk of security incidents from targeted email attacks?
A. Implement a data loss prevention (DLP) system
B. Disable all incoming cloud mail services
C. Conduct awareness training across the organization
D. Require acknowledgment of the acceptable use policy
Answer: (SHOW ANSWER)
Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks. Therefore, conducting awareness training across the organization is the correct answer.

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

NEW QUESTION: 454
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: 455
A global organization is planning to expand its operations into a new country with stricter data protection regulations than those in the headquarters' home country. Which of the following is the BEST approach for adopting these new requirements?
A. Adjust organization-wide security polices to align with regulations of the new country.
B. Procure cybersecurity insurance that covers potential breaches and incidents in the new country.
C. Ensure local operations comply with geographical data protection laws of the headquarters.
D. Work with legal to interpret the local regulatory requirements and implement applicable controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 456
Which of the following is the MOST important consideration when developing an approach to effectively contain security incidents?
A. Isolating systems impacted by incidents from the production environment
B. Mitigating reputational damage that may affect business
C. Minimizing financial losses that may result from outages

D. Assigning senior management accountability for incident containment

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 457

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: 458

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: 459
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: 460

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

A. Data governance

B. Business alignment

C. Information management

D. Regulatory compliance

Answer: (SHOW ANSWER)

NEW QUESTION: 461

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: 462

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

A. Verify that information security requirements are included in the contract.
B. Request customer references from the vendor.
C. Require vendors to complete information security questionnaires.
D. Review the results of the vendor's independent control reports.
Answer: (SHOW ANSWER)
Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.
Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting those requirements. The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.
Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment.
Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. References = CISM Review Manual 15th Edition, page 144 SaaS Security Risk and Challenges - ISACA1 SaaS Security Checklist & Assessment Questionnaire | LeanIX2 Risk Assessment Guide for Microsoft Cloud3

NEW QUESTION: 463
Which of the following is BEST used to determine the maturity of an information security program?
A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics
Answer: (SHOW ANSWER)
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes.

Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
References:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security- governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing- information-security

NEW QUESTION: 464
Of the following, who should be assigned as the owner of a newly identified risk related to an organization's new payroll system?
A. Head of IT department
B. Head of human resources (HR)
C. Information security manager
D. Data privacy officer
Answer: (SHOW ANSWER)

NEW QUESTION: 465
An information security manager learns that a risk owner has approved exceptions to replace key controls with weaker compensating controls to improve process efficiency. Which of the following should be the GREATEST concern?
A. Risk levels may be elevated beyond acceptable limits.
B. Security audits may report more high-risk findings.
C. The compensating controls may not be cost efficient.
D. Noncompliance with industry best practices may result.
Answer: A (LEAVE A REPLY)
Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

NEW QUESTION: 466
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.

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 467
An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?
A. Conduct an information security audit.
B. Validate the relevance of the information.
C. Perform a gap analysis.
D. Inform senior management
Answer: (SHOW ANSWER)
The information security manager's first course of action should be to validate the relevance of the information received from the threat intelligence service. This means verifying the source, credibility, accuracy, and timeliness of the information, as well as assessing the potential impact and likelihood of the threat for the organization. This will help the information security manager to determine the appropriate response and prioritize the actions to mitigate the threat. Conducting an information security audit, performing a gap analysis, and informing senior management are possible subsequent actions, but they are not the first course of action. An information security audit is a systematic and independent assessment of the effectiveness of the information security controls and processes. A gap analysis is a comparison of the current state of the information

security program with the desired state or best practices. Informing senior management is a communication activity that should be done after validating the information and assessing the risk.
References = CISM Review Manual, 16th Edition, pages 44-451; CISM Review Questions, Answers
& Explanations Manual, 10th Edition, page 632
The first step the information security manager should take upon learning of the potential threat is to validate the relevance of the information. This should involve researching the threat to evaluate its potential impact on the organization and to determine the accuracy of the threat intelligence. Once the information is validated, the information security manager can then take action, such as informing senior management, conducting an information security audit, or performing a gap analysis.

NEW QUESTION: 468
Which of the following is the BEST strategy when determining an organization's approach to risk treatment?
A. Advancing the maturity of existing controls based on risk tolerance
B. Prioritizing controls that directly mitigate the organization's most critical risks
C. Implementing risk mitigation controls that are considered quick wins
D. Implementing a one-size-fits-all set of controls across all organizational units
Answer: (SHOW ANSWER)
The best strategy for risk treatment is to prioritize controls that directly mitigate the organization's most critical risks. This aligns with a risk-based approach, where limited resources are directed toward areas with the highest business impact.
"Effective risk treatment involves prioritizing actions that address the most critical risks to the organization, considering impact and likelihood."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Advancing maturity or applying quick wins may help, but they are not as strategic or impactful as targeting top-priority risks.

NEW QUESTION: 469
An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?
A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.
Answer: (SHOW ANSWER)
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the

specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION: 470

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

Freecram.net

A. Review the risk monitoring plan.
B. Formally document the decision.
C. Review the regulations.
D. Advise the risk management team.
Answer: (SHOW ANSWER)
Since the identified risks are subject to regulatory requirements, and cannot simply be accepted without oversight, the information security manager should escalate the issue to the risk management team or higher authority to ensure proper governance.
"When risk acceptance contradicts regulatory requirements, it must be escalated to senior management or the risk function for resolution."
- CISM Review Manual 15th Edition, Chapter 1: Governance Responsibilities, Section: Risk Governance and Oversight*

NEW QUESTION: 471
Which of the following is the BEST reason to implement an information security architecture?
A. Fast-track the deployment of information security components.
B. Serve as a post-deployment information security road map.
C. Facilitate consistent implementation of security requirements.
D. Assess the cost-effectiveness of the integration.
Answer: (SHOW ANSWER)

NEW QUESTION: 472
Which of the following should be updated FIRST to account for new regulatory requirements that impact current information security controls?
A. Risk register
B. Information security policy
C. Business impact analysis (BIA)
D. Control matrix

Answer: (SHOW ANSWER)

NEW QUESTION: 473
In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?
A. Ownership of security
B. Compliance with policies
C. Auditability of systems
D. Allocation of training resources
Answer: (SHOW ANSWER)
Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks.
References: https://www.isaca.org/credentialing/cism
https://www.nist.gov/publications/information-security- handbook-guide-managers

NEW QUESTION: 474
In which cloud model does the cloud service buyer assume the MOST security responsibility?
A. Disaster Recovery as a Service (DRaaS)
B. Infrastructure as a Service (IaaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)
Answer: (SHOW ANSWER)
Infrastructure as a Service (IaaS) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment.
In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or

ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page
140-1411

NEW QUESTION: 475
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: 476
Prior to conducting a forensic examination, an information security manager should:
A. boot the original hard disk on a clean system.
B. create an image of the original data on new media.
C. duplicate data from the backup media.
D. shut down and relocate the server.
Answer: (SHOW ANSWER)
= A forensic examination is a process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable. The first step in conducting a forensic examination is to create an image of the original data on new media, such as a hard disk, a CD-ROM, or a USB drive. This is done to ensure that the original data is not altered, damaged, or destroyed during the examination. An image is an exact copy of the data, including the file system, the slack space, and the deleted files. Creating an image also allows the examiner to

work on a duplicate of the data, rather than the original, which may be needed as evidence in court. Booting the original hard disk on a clean system is not a good practice, as it may change the data on the disk, such as the timestamps, the registry entries, and the log files. Duplicating data from the backup media is not sufficient, as the backup media may not contain all the data that is relevant to the investigation, such as the deleted files, the temporary files, and the swap files. Shutting down and relocating the server is not advisable, as it may cause data loss, corruption, or tampering. The server should be kept running and isolated from the network until an image is created. References = CISM Review Manual 15th Edition, page 204-205.
Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

NEW QUESTION: 477
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 provide the response team with expert training on evidence handling
B. To prevent evidence from being disclosed to any internal staff members
C. To validate the incident response process
D. To ensure evidence is handled by qualified resources
Answer: (SHOW ANSWER)

NEW QUESTION: 478
Which of the following parties should be responsible for determining access levels to an application that processes client information?
A. The business client
B. The information security tear
C. The identity and access management team
D. Business unit management
Answer: (SHOW ANSWER)
The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.

The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

NEW QUESTION: 479
A global organization is developing an incident response team. The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events. Which of the following BEST supports these objectives?
A. Virtual incident response team
B. Distributed incident response team
C. Outsourced incident response team
D. Centralized incident response team
Answer: (SHOW ANSWER)
A centralized incident response team ensures consistent communication, coordination, and a unified approach to managing incidents across the organization.
"A centralized incident response team provides a consistent and coordinated approach to incident handling and ensures that management is kept informed."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Organization Models*

NEW QUESTION: 480
What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?
Freecram.net
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: 481
Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?
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.

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 482
Which of the following is a PRIMARY function of an incident response team?
A. To provide a risk assessment for zero-day vulnerabilities
B. To provide effective incident mitigation
C. To provide a business impact analysis (BIA)
D. To provide a single point of contact for critical incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 483
Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?
A. Security information and event management (SIEM)
B. Extended detection and response (XDR)
C. Endpoint detection and response (EDR)
D. Network intrusion detection system (NIDS)
Answer: (SHOW ANSWER)
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

NEW QUESTION: 484
Which of the following is the BEST method for determining whether new risks exist in legacy systems?
A. Frequent updates to the risk register
B. Regularly scheduled security audits
C. Frequent security architecture reviews
D. Regularly scheduled risk assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 485

Which of the following BEST indicates the effectiveness of the vendor risk management process?
A. Increase in the percentage of vendors certified to a globally recognized security standard
B. Increase in the percentage of vendors with a completed due diligence review
C. Increase in the percentage of vendors conducting mandatory security training
D. Increase in the percentage of vendors that have reported security breaches
Answer: A (LEAVE A REPLY)
This answer best indicates the effectiveness of the vendor risk management process because it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices.
A globally recognized security standard, such as ISO 27001, NIST CSF, or COBIT, provides a comprehensive and objective framework for assessing and improving the security posture and performance of vendors.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security requirements and expectations for third-party products and services are defined, communicated, and enforced" and that "the information security manager should verify that the third parties have implemented adequate security controls and practices, and that they comply with applicable standards and regulations" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Increase in the percentage of vendors certified to a globally recognized security standard is the correct answer because it best indicates the effectiveness of the vendor risk management process, as it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices" (p. 63). Additionally, the article Vendor Risk Management Demystified from the ISACA Journal 2015 states that "a globally recognized security standard provides a common language and framework for evaluating and improving the security posture and performance of vendors" and that "a vendor certification to a globally recognized security standard can help to reduce the risk of security breaches, increase the trust and confidence of customers and stakeholders, and enhance the reputation and competitiveness of the vendor" (p. 3

NEW QUESTION: 486
Which of the following is MOST important for building 4 robust information security culture within an organization?
A. Mature information security awareness training across the organization
B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies
Answer: (SHOW ANSWER)
= Mature information security awareness training across the organization is the most important factor for building a robust information security culture, because it helps to educate and motivate

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

NEW QUESTION: 487
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 avoid redundant controls
C. To align with emerging risk
D. To address end-user control complaints
Answer: (SHOW ANSWER)

NEW QUESTION: 488
An organization is planning to outsource the execution of its disaster recovery activities. Which of the following would be MOST important to include in the outsourcing agreement?
A. Definition of when a disaster should be declared
B. Requirements for regularly testing backups
C. Recovery time objectives (RTOs)

D. The disaster recovery communication plan

Answer: (SHOW ANSWER)

The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on the business impact analysis (BIA) and the risk assessment, and they reflect the business continuity requirements and expectations of the organization. By including the RTOs in the outsourcing agreement, the organization can ensure that the service provider is aware of and committed to meeting the agreed service levels and minimizing the downtime and losses in the event of a disaster. The other options are not as important as the RTOs, although they may be relevant and useful to include in the outsourcing agreement depending on the scope and nature of the disaster recovery services. References = CISM Review Manual 15th Edition, page 2471; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1033

NEW QUESTION: 489

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

A. Requirement for regular information security awareness

B. Right-to-audit clause

C. Service level agreement (SLA)

D. Requirement to comply with corporate security policy

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 490

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: 491
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: 492
Which of the following is the PRIMARY advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program?
A. It offers the organization flexible deployment options using cloud infrastructure.
B. It allows the organization to prioritize its core operations.
C. It is more secure than traditional data backup architecture.
D. It allows the use of a professional response team at a lower cost.
Answer: (SHOW ANSWER)
The primary advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program is B. It allows the organization to prioritize its core operations. This is because DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster1. DRaaS can help the organization to prioritize its core operations by:
Reducing the need for provisioning and maintaining its own off-site disaster recovery environment, which can be costly, complex, and resource-intensive12 Enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers, which can minimize the downtime, data loss, and business disruption12 Providing the organization with flexible and scalable deployment options, such as on-demand, pay-per-use, or subscription-based models, that can meet its changing business needs and budget12 Leveraging the expertise, experience, and best practices of the service provider, who can handle the disaster recovery planning, testing, and execution, and ensure compliance with the relevant standards and regulations12 DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. DRaaS can help the organization to prioritize its core operations by reducing the need for provisioning and maintaining its own off-site disaster recovery environment, enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment, providing the organization with flexible and scalable deployment options, and leveraging the expertise, experience, and best practices of the service provider. (From CISM Manual or related resources)

NEW QUESTION: 493
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: 494
When an organization lacks internal expertise to conduct highly technical forensics investigations, what is the BEST way to ensure effective and timely investigations following an information security incident?
A. Ensure the incident response policy allows hiring a forensics firm.
B. Purchase forensic standard operating procedures.
C. Retain a forensics firm prior to experiencing an incident.
D. Provide forensics training to the information security team.
Answer: (SHOW ANSWER)

NEW QUESTION: 495
When updating the information security policy to accommodate a new regulation, the information security manager should FIRST:
A. Review key risk indicators (KRIs)
B. Perform a gap analysis
C. Consult process owners
D. Update key performance indicators (KPIs)
Answer: (SHOW ANSWER)
A gap analysis identifies the differences between current practices and the new regulatory requirements, ensuring targeted and effective policy updates.
"Performing a gap analysis is critical to identify the areas where the current policy falls short of new regulatory requirements."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance* ISACA practice questions confirm that a gap analysis is the foundational step before engaging stakeholders or updating policies.

NEW QUESTION: 496
Which of the following roles has the PRIMARY responsibility to ensure the operating effectiveness of IT controls?
A. Risk owner

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

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/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 497
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: 498
For event logs to be acceptable for incident investigation, which of the following is the MOST important consideration to establish chain of evidence?
A. Administrator log access
B. Available forensic tools
C. Time clock synchronization
D. Centralized logging
Answer: (SHOW ANSWER)

NEW QUESTION: 499
Which of the following should be the FIRST step in patch management procedures when receiving an emergency security patch?
A. Schedule patching based on the criticality.
B. Install the patch immediately to eliminate the vulnerability.
C. Conduct comprehensive testing of the patch.
D. Validate the authenticity of the patch.
Answer: (SHOW ANSWER)
Validating the authenticity of the patch is the first step in patch management procedures when receiving an emergency security patch, as it helps to ensure that the patch is genuine and not malicious. Validating the authenticity of the patch can be done by verifying the source, signature, checksum, or certificate of the patch, and comparing it with the information provided by the software vendor or manufacturer. Installing an unverified patch may introduce malware, compromise the system, or cause unexpected errors or conflicts.
References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.42; Practical Patch Management and Mitigation1; Vulnerability and patch management in the CISSP exam3

NEW QUESTION: 500
Which of the following is the BEST way to evaluate the effectiveness of physical and environmental security controls implemented for fire-related disasters?
Freecram.net
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: 501
Which of the following metrics would provide an accurate measure of an information security program's performance?
A. A collection of quantitative indicators that are compared against industry benchmarks
B. A combination of qualitative and quantitative trends that enable decision making
C. A collection of qualitative indicators that accurately measure security exceptions
D. A single numeric score derived from various measures assigned to the security program
Answer: (SHOW ANSWER)

NEW QUESTION: 502
Which of the following would BEST mitigate accidental data loss events?
A. Conduct periodic user awareness training.
B. Obtain senior management support for the information security strategy.
C. Conduct a data loss prevention (DLP) audit.
D. Enforce a data hard drive encryption policy.
Answer: A (LEAVE A REPLY)
Conducting periodic user awareness training is the best way to mitigate accidental data loss events because it can educate the users on the causes, consequences, and prevention of data loss, and increase their awareness of the security policies and procedures of the organization. User awareness training can also help users to identify and report potential data loss incidents, and to adopt good practices such as backing up data, encrypting data, and using secure channels for data transmission and storage.
References: The article Mistakes Happen-Mitigating Unintentional Data Loss from the ISACA Journal 2018 states that "user awareness training is the most effective way to prevent unintentional data loss" and that "user awareness training should include information on the types and sources of data loss, the impact and cost of data loss, the legal and regulatory requirements for data protection, the organization's data security policies and procedures, the roles and responsibilities of users in data security, the best practices and tools for data security, and the reporting and escalation process for data loss incidents" (p. 2)1. The Data Spill Management Guide from the Cyber.gov.au website also states that "user awareness training is an important preventative measure to reduce the likelihood of data spills" and that "user awareness training

should cover topics such as data classification, data handling, data storage, data transmission, data disposal, and data spill reporting" (p. 2)

NEW QUESTION: 503
Which of the following BEST helps to enable the desired information security culture within an organization?
A. Information security awareness training and campaigns
B. Effective information security policies and procedures
C. Delegation of information security roles and responsibilities
D. Incentives for appropriate information security-related behavior
Answer: (SHOW ANSWER)
Information security awareness training and campaigns are the best way to enable the desired information security culture within an organization because they help to educate, motivate and influence the behavior and attitude of the employees towards information security. They also help to raise the awareness of the risks, threats and best practices of information security among the staff and stakeholders.
References = Organizational Culture for Information Security: A Systemic Perspective on the Articulation of Human, Cultural and Social Systems, CISM Exam Content Outline

NEW QUESTION: 504
Which of the following is the MOST effective way to detect information security incidents?
A. Periodic analysis of security event log records
B. Real-time monitoring of network activity
C. Threshold settings on key risk indicators (KRIs)
D. Implementation of regular security awareness programs
Answer: (SHOW ANSWER)

NEW QUESTION: 505
The PRIMARY reason to properly classify information assets is to determine:
A. the business impact if assets are compromised.
B. appropriate encryption strength using a risk-based approach.
C. user access levels based on the need to know.
D. the appropriate protection based on sensitivity.
Answer: (SHOW ANSWER)

NEW QUESTION: 506
An online bank identifies a successful network attack in progress. The bank should FIRST:
A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (PII) is compromised.
D. shut down the entire network.

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

NEW QUESTION: 507
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?
A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.
Answer: (SHOW ANSWER)
Defining information security requirements and processes is the FIRST thing that the information security manager should do to support the initiative of utilizing Software as a Service (SaaS) and selecting a vendor.
This is because information security requirements and processes provide the basis for evaluating and comparing the SaaS vendors and solutions, as well as for ensuring the alignment of the SaaS services with the organization's security objectives, policies, and standards. Information security requirements and processes should include aspects such as data protection, access control, encryption, authentication, authorization, audit, compliance, incident response, disaster recovery, and service level agreements12. Reviewing independent security assessment reports for each vendor (A) is a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Independent security assessment reports can provide valuable information about the security posture, practices, and performance of the SaaS vendors and solutions, such as their compliance with industry standards, frameworks, and regulations, their vulnerability and risk management, and their security testing and auditing results. However, reviewing independent security assessment reports should be done after defining the information security requirements and processes, which can help to determine the scope, criteria, and expectations for the security assessment12. Benchmarking each vendor's services with industry best practices (B) is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Benchmarking each vendor's services with industry best practices can help to measure and compare the quality, performance, and value of

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

NEW QUESTION: 508
Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?
A. Impact on information security program
B. Cost of controls
C. Impact to business function
D. Cost to replace
Answer: (SHOW ANSWER)
The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.
Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset. Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization. References = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693 When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of

the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture.
Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

NEW QUESTION: 509
Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?
A. Low number of false positives
B. Low number of false negatives
C. High number of false positives
D. High number of false negatives
Answer: (SHOW ANSWER)
A false negative is a security incident that was not detected by the SIEM system, which presents the greatest risk as it allows attackers to compromise the organization's assets and data without being noticed or stopped.
A high number of false negatives can indicate that the SIEM system is not configured properly, has insufficient data sources, or lacks effective analytics and correlation rules. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 510
An employee of an organization has reported losing a smartphone that contains sensitive information
The BEST step to address this situation is to:
Freecram.net
A. disable the user's access to corporate resources.
B. terminate the device connectivity.
C. remotely wipe the device
D. escalate to the user's management
Answer: (SHOW ANSWER)
The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user' s management, may not be effective or timely enough to secure the sensitive information on the device.
References:
https://www.security.org/resources/protect-data-lost-device/
https://support.google.com/android/answer/6160491?hl=en

https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

NEW QUESTION: 511
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

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 512
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: 513
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: 514
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: (SHOW ANSWER)

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: 515
An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?
A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.
Answer: (SHOW ANSWER)
A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:
* It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.
* It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
* It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
* It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
* It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.
The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because

they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. References = 1: What is a Gap Analysis? | Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:
1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.
infosecinstitute.com+2 more

NEW QUESTION: 516
Business objectives and organizational risk appetite are MOST useful inputs to the development of information security:
A. key performance indicators (KPIs).
B. standards.
C. risk assessments.
D. strategy.
Answer: (SHOW ANSWER)

NEW QUESTION: 517
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

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/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)