Isaca

Exam Questions CISM

Certified Information Security Manager

Passing Certification Exams Made Easy

NEW QUESTION 1
- (Topic 2)
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?

A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan

Answer: B

Explanation:
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 2
- (Topic 1)
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: D

Explanation:
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 3
- (Topic 1)
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

Explanation:
= 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 4
- (Topic 1)
Management decisions concerning information security investments will be MOST effective when they are based on:

A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,

Answer: C

Explanation:
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic

assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION 5
- (Topic 3)
A security incident has been reported within an organization When should an information security manager contact the information owner?

A. After the incident has been mitigated
B. After the incident has been confirmed.
C. After the potential incident has been togged
D. After the incident has been contained

Answer: B

Explanation:
= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

NEW QUESTION 6
- (Topic 3)
Which of the following metrics is MOST appropriate for evaluating the incident notification process?

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

Answer: D

Explanation:
Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.
References:
? https://www.atlassian.com/incident-management/kpis/common-metrics
? https://securityscorecard.com/blog/how-to-use-incident-response-metrics/
? https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan- Basics_508c.pdf

NEW QUESTION 7
- (Topic 3)
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

A. Authority of the subscriber to approve access to its data
B. Right of the subscriber to conduct onsite audits of the vendor
C. Commingling of subscribers' data on the same physical server
D. Escrow of software code with conditions for code release

Answer: A

Explanation:
Authority of the subscriber to approve access to its data is the greatest concern for an information security manager if omitted from the contract, as it may expose the subscriber's data to unauthorized or inappropriate access by the vendor or third parties. The subscriber should have the right to control who can access its data, for what purposes, and under what conditions. The contract should also specify the vendor's obligations to protect the confidentiality, integrity, and availability of the subscriber's data, and to notify the subscriber of any breaches or incidents.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2201; Drafting and Negotiating Effective Cloud Computing Agreements2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

NEW QUESTION 8
- (Topic 3)
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?

A. Configuration management
B. Risk management
C. Access control management
D. Change management

Answer: D

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

NEW QUESTION 9
- (Topic 3)
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

A. To facilitate the continuous improvement of the IT organization
B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan

Answer: B

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

NEW QUESTION 10
- (Topic 3)
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: D

Explanation:
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 11
- (Topic 1)
In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:

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

Answer: B

Explanation:
= 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 12
- (Topic 3)
Which of the following BEST facilitates the reporting of useful information about the effectiveness of the information security program?

A. Risk heat map.
B. Security benchmark report.
C. Security metrics dashboard.
D. Key risk indicators (KRIs).

Answer: C

Explanation:
A security metrics dashboard is a graphical representation of key performance indicators (KPIs) and key risk indicators (KRIs) that provide useful information about the effectiveness of the information security program. A security metrics dashboard can help communicate the value and performance of the information security program to senior management and other stakeholders, as well as identify areas for improvement and alignment with business objectives. A security metrics dashboard should be concise, relevant, timely, accurate, and actionable.
References = CISM Review Manual 16th Edition, page 163; CISM Review Questions, Answers & Explanations Manual 9th Edition, page 419.

NEW QUESTION 13
- (Topic 3)
When developing an information security strategy for an organization, which of the following is MOST helpful for understanding where to focus efforts?

A. Gap analysis
B. Project plans
C. Vulnerability assessment
D. Business impact analysis (BIA)

Answer: A

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

NEW QUESTION 14
- (Topic 2)
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: D

Explanation:
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 15
- (Topic 2)
An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?

A. Wipe and reset the endpoint device.
B. Isolate the endpoint device.
C. Power off the endpoint device.
D. Run a virus scan on the endpoint device.

Answer: B

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

NEW QUESTION 16
- (Topic 2)
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?

A. Patch management files
B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs

Answer: A

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

NEW QUESTION 17
- (Topic 2)
An organization is creating a risk mitigation plan that considers redundant power supplies to reduce the business risk associated with critical system outages.
Which type of control is being considered?

A. Preventive
B. Corrective
C. Detective
D. Deterrent

Answer: A

Explanation:
A preventive control is a type of control that aims to prevent or reduce the occurrence or impact of potential adverse events that can affect the organization's objectives and performance. Preventive controls are proactive measures that are implemented before an incident happens, and they are designed to address the root causes or sources of risk. Preventive controls can also help the organization to comply with the relevant laws, regulations, standards, and best practices regarding information security1.
An example of a preventive control is a redundant power supply, which is a backup or alternative source of power that can be used in case of a power outage or failure. A redundant power supply can reduce the business risk associated with critical system outages, which can result from power disruptions caused by natural disasters, technical faults, human errors, or malicious attacks. A redundant power supply can provide the following benefits for information security2:
? Maintain the availability and continuity of the critical systems and services that
depend on power, such as servers, databases, networks, or applications. A redundant power supply can ensure that the critical systems and services can operate normally or resume quickly after a power outage or failure, minimizing the downtime and data loss that can affect the organization's operations, customers, or reputation.
? Protect the integrity and reliability of the critical systems and data that are stored or processed by the power-dependent devices, such as computers, hard drives, or memory cards. A redundant power supply can prevent or reduce the damage or corruption of the critical systems and data that can be caused by sudden or unexpected power fluctuations, surges, or interruptions, which can compromise the accuracy, completeness, or consistency of the information.
? Enhance the resilience and redundancy of the power infrastructure and network that supports the critical systems and services. A redundant power supply can provide an alternative or backup route for power delivery and distribution, which can increase the flexibility and adaptability of the power infrastructure and network to cope with different scenarios or conditions of power supply or demand.
The other options are not the type of control that is being considered by the organization. A corrective control is a type of control that aims to restore or recover the normal state or function of the affected systems or processes after an incident has occurred. A corrective control is a reactive measure that is implemented during or after an incident, and it is designed to address the consequences or impacts of risk. A corrective control can also help the organization to learn from the incident and improve its information security practices1. An example of a corrective control is a backup or restore system, which is a method of creating and restoring copies of the system or data that have been lost or damaged due to an incident.
A detective control is a type of control that aims to identify or discover the occurrence or existence of an incident or a deviation from the expected or desired state or behavior of the systems or processes. A detective control is a monitoring or auditing measure that is implemented during or after an incident, and it is designed to provide information or evidence of risk. A detective control can also help the organization to analyze or investigate the incident and determine the root cause or source of risk1. An example of a detective control is a log or alert system, which is a tool of recording or reporting the activities or events that have occurred or are occurring within the systems or processes.
A deterrent control is a type of control that aims to discourage or dissuade the potential perpetrators or sources of risk from initiating or continuing an incident or an attack. A deterrent control is a psychological or behavioral measure that is implemented before or during an incident, and it is designed to influence or manipulate

the motivation or intention of risk. A deterrent control can also help the organization to reduce the likelihood or frequency of incidents or attacks1. An example of a deterrent control is a warning or notification system, which is a method of communicating or displaying the consequences or penalties of violating the information security policies or rules. References = Risk Control Techniques: Preventive, Corrective, Directive, And …, Learn Different types of Security Controls in CISSP - Eduonix Blog

NEW QUESTION 18
- (Topic 2)
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: C

Explanation:
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 19
- (Topic 3)
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: B

Explanation:
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 20
- (Topic 3)
Which of the following will BEST enable an effective information asset classification process?

A. Including security requirements in the classification process
B. Analyzing audit findings
C. Reviewing the recovery time objective (RTO) requirements of the asset
D. Assigning ownership

Answer: D

Explanation:
Assigning ownership is the best way to enable an effective information asset classification process, as it establishes the authority and responsibility for the information asset and its protection. The owner of the information asset should be involved in the classification process, as they have the best knowledge of the value, sensitivity, and criticality of the asset, as well as the impact of its loss or compromise. The owner should also ensure that the asset is properly labeled, handled, and secured according to its classification level. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Information Asset and Security Classification Procedure1, section 3.1.

NEW QUESTION 21
- (Topic 3)
An organization plans to leverage popular social network platforms to promote its products and services. Which of the following is the BEST course of action for the information security manager to support this initiative?

A. Establish processes to publish content on social networks.
B. Assess the security risk associated with the use of social networks.
C. Conduct vulnerability assessments on social network platforms.
D. Develop security controls for the use of social networks.

Answer: B

Explanation:
The best course of action for the information security manager to support the initiative of leveraging popular social network platforms to promote the organization's products and services is to assess the security risk associated with the use of social networks. Security 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 security risk assessment, the information security manager can provide valuable input to the decision-making process regarding the benefits and costs of using social networks, as well as the appropriate security controls and mitigation strategies to reduce the risk to an acceptable level. The other options are not the best course of action, although they may be part of the security risk management process. Establishing processes to publish content on social networks is an operational task that should be performed after assessing the security risk and implementing the necessary controls. Conducting vulnerability assessments on social network platforms is a technical activity that may not be feasible or effective, as the organization does not have control over the platforms' infrastructure and configuration. Developing security controls for the use of social networks is a preventive measure that should be based on the results of the security risk assessment and aligned with the organization's risk appetite and tolerance

NEW QUESTION 22
- (Topic 3)
Which of the following should be the GREATEST consideration when determining the recovery time objective (RTO) for an in-house critical application, database, or server?

A. Impact of service interruption
B. Results of recovery testing
C. Determination of recovery point objective (RPO)
D. Direction from senior management

Answer: A

NEW QUESTION 23
- (Topic 3)
Which of the following control types should be considered FIRST for aligning employee behavior with an organization's information security objectives?

A. Administrative security controls
B. Technical security controls
C. Physical security controls
D. Access security controls

Answer: A

NEW QUESTION 24
- (Topic 3)
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: D

Explanation:
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 25
- (Topic 3)
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: B

Explanation:

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 26
- (Topic 3)
Which of the following is MOST important to the effectiveness of an information security program?

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

Answer: D

Explanation:
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 27
- (Topic 3)
Which of the following is the BEST way to reduce the risk of security incidents from targeted email attacks?

A. Implement a data loss prevention (DLP) system
B. Disable all incoming cloud mail services
C. Conduct awareness training across the organization
D. Require acknowledgment of the acceptable use policy

Answer: C

Explanation:
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 28
- (Topic 3)
Which of the following should be the FIRST step in developing an information security strategy?

A. Perform a gap analysis based on the current state
B. Create a roadmap to identify security baselines and controls.
C. Identify key stakeholders to champion information security.
D. Determine acceptable levels of information security risk.

Answer: A

Explanation:
The FIRST step in developing an information security strategy is to perform a gap analysis based on the current state of the organization's information security posture. A gap analysis is a systematic process of comparing the current state with the desired state and identifying the gaps or deficiencies that need to be addressed. A gap analysis helps to establish a baseline for the information security strategy, as well as to prioritize the actions and resources needed to achieve the strategic objectives. A gap analysis also helps to align the information security strategy with the organizational goals and strategies, as well as to ensure compliance with relevant standards and regulations. References = CISM Review Manual, 16th Edition, page 331; CISM Review Questions, Answers &

Explanations Manual, 10th Edition, page 162
first step in developing an information security strategy is to conduct a risk-aware and comprehensive inventory of your company's context, including all digital assets, employees, and vendors. Then you need to know about the threat environment and which types of attacks are a threat to your company1. This is similar to performing a gap analysis based on the current state3.

NEW QUESTION 29
- (Topic 3)
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: A

Explanation:
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 30
- (Topic 3)
Which of the following factors would have the MOST significant impact on an organization's information security governance mode?

A. Outsourced processes
B. Security budget
C. Number of employees
D. Corporate culture

Answer: D

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

NEW QUESTION 31
.....