Isaca

Exam Questions CISM

Certified Information Security Manager

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Topic 2)
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: A

Explanation:
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 2
- (Topic 2)
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: D

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

NEW QUESTION 3
- (Topic 1)
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: C

Explanation:
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 4
- (Topic 1)
Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?

A. The capabilities and expertise of the information security team
B. The organization's mission statement and roadmap
C. A prior successful information security strategy
D. The organization's information technology (IT) strategy

Answer: B

Explanation:
= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization’s mission statement and roadmap. The mission statement defines the organization’s purpose, vision, values, and goals, and the roadmap outlines the organization’s strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security

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

NEW QUESTION 5
- (Topic 1)
Which of the following will have the GREATEST influence on the successful adoption of an information security governance program?

A. Security policies
B. Control effectiveness
C. Security management processes
D. Organizational culture

Answer: D

Explanation:
Organizational culture is the set of shared values, beliefs, and norms that influence the way employees think, feel, and behave in the workplace. It affects how employees perceive the importance of information security, how they comply with security policies and procedures, and how they support security initiatives and goals. A strong security culture can foster a sense of ownership, responsibility, and accountability among employees, as well as a positive attitude toward security awareness and training. A weak security culture can lead to resistance, indifference, or hostility toward security efforts, as well as increased risks of human errors, negligence, or malicious actions. Therefore, organizational culture has the greatest influence on the successful adoption of an information security governance program, which requires the commitment and involvement of all levels of the organization. References = CISM Review Manual 15th Edition, page 30- 31. Learn more:

NEW QUESTION 6
- (Topic 1)
Which of the following BEST indicates that information assets are classified accurately?

A. Appropriate prioritization of information risk treatment
B. Increased compliance with information security policy
C. Appropriate assignment of information asset owners
D. An accurate and complete information asset catalog

Answer: A

Explanation:
The best indicator that information assets are classified accurately is appropriate prioritization of information risk treatment. Information asset classification is the process of assigning a level of sensitivity or criticality to information assets based on their value, impact, and legal or regulatory requirements. The purpose of information asset classification is to facilitate the identification and protection of information assets according to their importance and risk exposure. Therefore, if information assets are classified accurately, the organization can prioritize the information risk treatment activities and allocate the resources accordingly. The other options are not direct indicators of information asset classification accuracy, although they may be influenced by it. References = CISM Review Manual 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1031

NEW QUESTION 7
- (Topic 1)
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: A

Explanation:
= 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 8
- (Topic 1)
Which of the following is the BEST indication of an effective information security awareness training program?

A. An increase in the frequency of phishing tests
B. An increase in positive user feedback
C. An increase in the speed of incident resolution
D. An increase in the identification rate during phishing simulations

Answer: D

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

NEW QUESTION 9
- (Topic 1)
When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

A. best practices.
B. control framework
C. regulatory requirements.
D. cost-benefit analysis,

Answer: D

Explanation:
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 10
- (Topic 1)
Which of the following BEST supports information security management in the event of organizational changes in security personnel?

A. Formalizing a security strategy and program
B. Developing an awareness program for staff
C. Ensuring current documentation of security processes
D. Establishing processes within the security operations team

Answer: C

Explanation:
Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can

minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION 10
- (Topic 1)
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems

Answer: B

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

NEW QUESTION 14
- (Topic 1)
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

Explanation:
= 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 18
- (Topic 1)
An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?

A. Determine whether the organization can benefit from adopting the new standard.
B. Obtain legal counsel's opinion on the standard's applicability to regulations,
C. Perform a risk assessment on the new technology.
D. Review industry specialists’ analyses of the new standard.

Answer: A

Explanation:
= The first step that the information security manager should recommend when learning of a new standard related to an emerging technology is to determine whether the organization can benefit from adopting the new standard. This involves evaluating the business objectives, needs, and requirements of the organization, as well as the potential advantages, disadvantages, and challenges of implementing the new technology and the new standard. The information security manager should also consider the alignment of the new standard with the organization’s existing policies, procedures, and standards, as well as the impact of the new standard on the organization’s information security governance, risk management, program, and incident management. By conducting a preliminary analysis of the feasibility, suitability, and desirability of the new standard, the information security manager can provide a sound basis for further decision making and planning.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Standards, page 391; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 43, page 412.

NEW QUESTION 22
- (Topic 1)

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: A

Explanation:
= 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 26
- (Topic 1)
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: C

Explanation:
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 29
- (Topic 1)
Which of the following provides an information security manager with the MOST accurate indication of the organization's ability to respond to a cyber attack?

A. Walk-through of the incident response plan
B. Black box penetration test
C. Simulated phishing exercise
D. Red team exercise

Answer: D

Explanation:
A red team exercise is a simulated cyber attack conducted by a group of ethical hackers or security experts (the red team) against an organization’s network, systems, and staff (the blue team) to test the organization’s ability to detect, respond, and recover from a real cyber attack. A red team exercise provides an information security manager with the most accurate indication of the organization’s ability to respond to a cyber attack, because it mimics the tactics, techniques, and procedures of real threat actors, and challenges the organization’s security posture, incident response plan, and security awareness in a realistic and adversarial scenario12. A red team exercise can measure the following aspects of the organization’s cyber attack response capability3:
? The effectiveness and efficiency of the security controls and processes in preventing, detecting, and mitigating cyber attacks
? The readiness and performance of the incident response team and other stakeholders in following the incident response plan and procedures
? The communication and coordination among the internal and external parties involved in the incident response process
? The resilience and recovery of the critical assets and functions affected by the cyber attack
? The lessons learned and improvement opportunities identified from the cyber attack simulation
The other options, such as a walk-through of the incident response plan, a black box penetration test, or a simulated phishing exercise, are not as accurate as a red team exercise in indicating the organization’s ability to respond to a cyber attack, because they have the following limitations4 :
? A walk-through of the incident response plan is a theoretical and hypothetical exercise that involves reviewing and discussing the incident response plan and procedures with the relevant stakeholders, without actually testing them in a live environment. A walk-through can help to familiarize the participants with the

incident response roles and responsibilities, and to identify any gaps or inconsistencies in the plan, but it cannot measure the actual performance and effectiveness of the incident response process under a real cyber attack scenario.
? A black box penetration test is a technical and targeted exercise that involves testing the security of a specific system or application, without any prior knowledge or access to its internal details or configuration. A black box penetration test can help to identify the vulnerabilities and weaknesses of the system or application, and to simulate the perspective and behavior of an external attacker, but it cannot test the security of the entire network or organization, or the response of the incident response team and other stakeholders to a cyber attack.
? A simulated phishing exercise is a social engineering and awareness exercise that involves sending fake emails or messages to the organization's staff, to test their ability to recognize and report phishing attempts. A simulated phishing exercise can help to measure the level of security awareness and training of the staff, and to simulate one of the most common cyber attack vectors, but it cannot test the security of the network or systems, or the response of the incident response team and other stakeholders to a cyber attack.
References = 1: What is a Red Team Exercise? | Redscan 2: Red Team vs Blue Team: How They Differ and Why You Need Both | CISA 3: Red Team Exercises: What They Are and How to Run Them | Rapid7 4: What is a Walkthrough Test? | Definition and Examples | ISACA : Penetration Testing Types: Black Box, White Box, and Gray Box | CISA

NEW QUESTION 30
- (Topic 1)
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

Explanation:
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 35
- (Topic 1)
The MOST appropriate time to conduct a disaster recovery test would be after:

A. major business processes have been redesigned.
B. the business continuity plan (BCP) has been updated.
C. the security risk profile has been reviewed
D. noncompliance incidents have been filed.

Answer: B

Explanation:
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 36
- (Topic 1)
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: A

Explanation:
= 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 38
- (Topic 1)
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials

Answer: B

Explanation:
= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.
References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

NEW QUESTION 43
- (Topic 1)
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: B

Explanation:
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 46
- (Topic 1)
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

Explanation:
= 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 48
- (Topic 1)
A recovery point objective (RPO) is required in which of the following?

A. Disaster recovery plan (DRP)

B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)

Answer: A

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

NEW QUESTION 50
- (Topic 1)
An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

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

Answer: A

Explanation:
The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization. Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.
Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.
Inviting IT members into regular procurement team meetings to influence best practice © is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.
Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, Page 141-1421

NEW QUESTION 52
- (Topic 1)
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: B

Explanation:
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 53
- (Topic 1)
Which of the following is the BEST way to achieve compliance with new global regulations related to the protection of personal information?

A. Execute a risk treatment plan.
B. Review contracts and statements of work (SOWs) with vendors.
C. Implement data regionalization controls.
D. Determine current and desired state of controls.

Answer: D

Explanation:
The best way to achieve compliance with new global regulations related to the protection of personal information is to determine the current and desired state of controls, as this helps the information security manager to identify the gaps and requirements for compliance, and to prioritize and implement the necessary actions and measures to meet the regulatory standards. The current state of controls refers to the existing level of protection and compliance of the personal information, while the desired state of controls refers to the target level of protection and compliance that is required by the new regulations. By comparing the current and desired state of controls, the information security manager can assess the maturity and effectiveness of the information security program, and plan and execute a risk treatment plan to address the risks and issues related to the protection of personal information. Executing a risk treatment plan, reviewing contracts and statements of work (SOWs) with vendors, and implementing data regionalization controls are also important, but not as important as determining the current and desired state of controls, as they are dependent on the outcome of the gap analysis and the risk assessment, and may not be sufficient or appropriate to achieve compliance with the new regulations. References = CISM Review Manual 2023, page 491; CISM Review Questions, Answers & Explanations Manual 2023, page 352; ISACA CISM - iSecPrep, page 203

NEW QUESTION 56
- (Topic 1)
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology

Answer: B

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

NEW QUESTION 58
- (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 61
- (Topic 1)
Which of the following is MOST important to consider when determining asset valuation?

A. Asset recovery cost
B. Asset classification level
C. Cost of insurance premiums

D. Potential business loss

Answer: D

Explanation:
Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important as potential business loss, as they do not capture the full value of the asset to the organization. References = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

NEW QUESTION 62
- (Topic 1)
If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:

A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.

Answer: B

Explanation:
Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court. The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12. Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server-backup utilities © is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks involved in the incident, but it may also introduce changes or errors that could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12. Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files, or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4: Information Security Incident Management (ISIM) [2022 update]2

NEW QUESTION 65
- (Topic 1)
An information security manager developing an incident response plan MUST ensure it includes:

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

Answer: B

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

NEW QUESTION 67
- (Topic 1)
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: A

Explanation:
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 72
- (Topic 1)
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: C

Explanation:
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 73
- (Topic 1)
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

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

Answer: B

Explanation:
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION 74
- (Topic 1)
When properly implemented, secure transmission protocols protect transactions:

A. from eavesdropping.
B. from denial of service (DoS) attacks.
C. on the client desktop.

D. in the server's database.

Answer: A

Explanation:
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 75
- (Topic 1)
Which of the following is MOST important to include in a post-incident review following a data breach?

A. An evaluation of the effectiveness of the information security strategy
B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom

Answer: B

Explanation:
= A post-incident review is a process of analyzing and learning from a security incident, such as a data breach, to improve the security posture and resilience of an organization. A post-incident review should include the following elements12:
? A clear and accurate description of the incident, including its scope, impact, timeline, root cause, and contributing factors.
? A detailed assessment of the effectiveness and efficiency of the incident response process, including the roles and responsibilities, communication channels, coordination mechanisms, escalation procedures, tools and resources, documentation, and reporting.
? An evaluation of the adequacy of existing controls, such as policies, standards, procedures, technical measures, awareness, and training, to prevent, detect, and mitigate similar incidents in the future.
? A list of actionable recommendations and improvement plans, based on the lessons learned and best practices, to address the identified gaps and weaknesses in the security strategy, governance, risk management, and incident management.
? A follow-up and monitoring mechanism to ensure the implementation and verification of the recommendations and improvement plans.
The most important element to include in a post-incident review following a data breach is the evaluation of the adequacy of existing controls, because it directly relates to the security objectives and requirements of the organization, and provides the basis for enhancing the security posture and resilience of the organization. Evaluating the existing controls helps to identify the vulnerabilities and risks that led to the data breach, and to determine the appropriate corrective and preventive actions to reduce the likelihood and impact of similar incidents in the future. Evaluating the existing controls also helps to align the security strategy and governance with the business goals and objectives, and to ensure the compliance with legal, regulatory, and contractual obligations.
The other elements, such as an evaluation of the effectiveness of the information security strategy, documentation of regulatory reporting requirements, and a review of the forensics chain of custody, are also important, but not as important as the evaluation of the existing controls. An evaluation of the effectiveness of the information security strategy is a broader and more strategic activity that may not be directly relevant to the specific incident, and may require more time and resources to conduct. Documentation of regulatory reporting requirements is a necessary and mandatory task, but it does not provide much insight or value for improving the security posture and resilience of the organization. A review of the forensics chain of custody is a technical and procedural activity that ensures the integrity and admissibility of the digital evidence collected during the incident investigation, but it does not address the root cause or the mitigation of the incident.
References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM Review Manual 15th Edition, page 147

NEW QUESTION 78
- (Topic 1)
Which of the following activities MUST be performed by an information security manager for change requests?

A. Perform penetration testing on affected systems.
B. Scan IT systems for operating system vulnerabilities.
C. Review change in business requirements for information security.
D. Assess impact on information security risk.

Answer: D

NEW QUESTION 83
- (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 88
- (Topic 1)
Who is BEST suited to determine how the information in a database should be classified?

A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner

Answer: D

Explanation:
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements. Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331

NEW QUESTION 92
- (Topic 1)
What is the BEST way to reduce the impact of a successful ransomware attack?

A. Perform frequent backups and store them offline.
B. Purchase or renew cyber insurance policies.
C. Include provisions to pay ransoms ih the information security budget.
D. Monitor the network and provide alerts on intrusions.

Answer: A

Explanation:
Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself. Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

NEW QUESTION 94
- (Topic 1)
When developing an asset classification program, which of the following steps should be completed FIRST?

A. Categorize each asset.
B. Create an inventor
C. &
D. Create a business case for a digital rights management tool.
E. Implement a data loss prevention (OLP) system.

Answer: B

Explanation:
Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified. An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12. Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12. Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset
classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. References = 1: CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4: What is Data Loss Prevention (DLP)? - Definition from Techopedia4

NEW QUESTION 98
- (Topic 1)
Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?

A. Availability of web application firewall logs.
B. Capability of online virtual machine analysis
C. Availability of current infrastructure documentation
D. Capability to take a snapshot of virtual machines

Answer: D

Explanation:
A snapshot is a point-in-time copy of the state of a virtual machine (VM) that can be used to restore the VM to a previous state in case of a security incident or a disaster. A snapshot can capture the VM's disk, memory, and device configuration, allowing for a quick and easy recovery of the VM's data and functionality. Snapshots can also be used to create backups, clones, or replicas of VMs for testing, analysis, or migration purposes. Snapshots are a common service offering in Infrastructure as a Service (IaaS) models, where customers can provision and manage VMs on demand from a cloud service provider (CSP). A CSP that offers the capability to take snapshots of VMs can assist customers when recovering from a security incident by providing them with the following benefits12:
? Faster recovery time: Snapshots can reduce the downtime and data loss caused by a security incident by allowing customers to quickly revert their VMs to a known good state. Snapshots can also help customers avoid the need to reinstall or reconfigure their VMs after an incident, saving time and resources.
? Easier incident analysis: Snapshots can enable customers to perform online or offline analysis of their VMs after an incident, without affecting the production environment. Customers can use snapshots to examine the VM's disk, memory, and logs for evidence of compromise, root cause analysis, or forensic investigation. Customers can also use snapshots to test and validate their incident response plans or remediation actions before applying them to the production VMs.
? Enhanced security posture: Snapshots can improve the security posture of customers by enabling them to implement best practices such as backup and restore, disaster recovery, and business continuity. Snapshots can help customers protect their VMs from accidental or malicious deletion, corruption, or modification, as well as from environmental or technical disruptions. Snapshots can also help customers comply with regulatory or contractual requirements for data retention, availability, or integrity. References = What is Disaster Recovery as a Service? | CSA - Cloud Security Alliance, What Is Cloud Incident Response (IR)? CrowdStrike

NEW QUESTION 103
- (Topic 1)
Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?

A. A capability and maturity assessment
B. Detailed analysis of security program KPIs
C. An information security dashboard
D. An information security risk register

Answer: C

Explanation:
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 108
- (Topic 1)
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: D

Explanation:
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 109
- (Topic 1)
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: B

Explanation:
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 111
- (Topic 1)
Which of the following is MOST critical when creating an incident response plan?

A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Documenting incident notification and escalation processes
D. Aligning with the risk assessment process

Answer: C

Explanation:
= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION 112
- (Topic 1)
Which of the following is the BEST indication ofa successful information security culture?

A. Penetration testing is done regularly and findings remediated.

B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.

Answer: B

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

NEW QUESTION 114
- (Topic 1)
Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Business contingency plan

Answer: C

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

NEW QUESTION 115
- (Topic 3)
Which of the following is MOST important when designing security controls for new cloud- based services?

A. Evaluating different types of deployment models according to the associated risks
B. Understanding the business and IT strategy for moving resources to the cloud
C. Defining an incident response policy to protect data moving between onsite and cloud applications
D. Performing a business impact analysis (BIA) to gather information needed to develop recovery strategies

Answer: B

Explanation:
The most important factor when designing security controls for new cloud-based services is to understand the business and IT strategy for moving resources to the cloud. This will help to align the security controls with the business objectives, requirements, and risks, and to select the appropriate cloud service delivery and deployment models. The security controls should also be based on the shared responsibility model, which defines the roles and responsibilities of the cloud service provider and the cloud customer in ensuring the security of the cloud environment. Evaluating different types of deployment models, defining an incident response policy, and performing a business impact analysis are also important activities, but they should be done after understanding the business and IT strategy.
References = CISM Review Manual, 16th Edition eBook1, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 141-142.

NEW QUESTION 117
- (Topic 3)
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?

A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.

Answer: C

Explanation:
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third- party cybersecurity incident management

NEW QUESTION 122
- (Topic 3)
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: D

Explanation:
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 124
- (Topic 3)
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: D

Explanation:
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 127
- (Topic 3)
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: D

Explanation:
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 129
- (Topic 3)
Which of the following is the MOST effective way to ensure the security of services and solutions delivered by third-party vendors?

A. Integrate risk management into the vendor management process.
B. Conduct security reviews on the services and solutions delivered.
C. Review third-party contracts as part of the vendor management process.
D. Perform an audit on vendors' security controls and practices.

Answer: A

Explanation:
Integrating risk management into the vendor management process is the most effective way to ensure the security of services and solutions delivered by third-party vendors, as it enables the organization to identify, assess, treat, and monitor the risks associated with outsourcing. Risk management should be applied

throughout the vendor life cycle, from selection, contracting, onboarding, monitoring, to termination. Risk management also helps the organization to define the security requirements, expectations, and responsibilities for the vendors, and to evaluate their performance and compliance. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2; Preparing Your First Supplier Audit Plan1.

NEW QUESTION 133
- (Topic 3)
When developing a categorization method for security incidents, the categories MUST:

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

Answer: C

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

NEW QUESTION 136
- (Topic 3)
Which of the following BEST indicates that an information security governance framework has been successfully implemented?

A. The framework aligns internal and external resources.
B. The framework aligns security processes with industry best practices.
C. The framework aligns management and other functions within the security organization.
D. The framework includes commercial off-the-shelf security solutions.

Answer: A

Explanation:
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 137
- (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 140
- (Topic 3)
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: A

Explanation:
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 142
- (Topic 3)
For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:

A. consistent security.
B. comprehensive audits
C. a security-aware culture
D. compliance with policy

Answer: A

Explanation:
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 147
- (Topic 3)
Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?

A. Residual risk
B. Regulatory requirements
C. Risk tolerance
D. Control objectives

Answer: C

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

NEW QUESTION 150
- (Topic 1)
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: D

Explanation:
= 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 152
- (Topic 3)
Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?

A. Enforce the local regulation.
B. Obtain legal guidance.
C. Enforce the organization's information security policy.
D. Obtain an independent assessment of the regulation.

Answer: B

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

NEW QUESTION 154
- (Topic 3)
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?

A. Ensuring hashing of administrator credentials
B. Enforcing service level agreements (SLAs)
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process

Answer: C

Explanation:
Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

NEW QUESTION 155
- (Topic 3)
During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption, unauthorized alterations, and errors?

A. Configuration management
B. Password management
C. Change management
D. Version management

Answer: C

Explanation:
Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION 159
- (Topic 3)
Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?

A. Alignment with industry benchmarks
B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget

Answer: B

Explanation:
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 160
.....

Relate Links

100% Pass Your CISM Exam with Exambible Prep Materials

https://www.exambible.com/CISM-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/