Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
- (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 2
- (Topic 1)
The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

A. enhance the organization's antivirus controls.
B. eliminate the risk of data loss.
C. complement the organization's detective controls.
D. reduce the need for a security awareness program.

Answer: C

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

NEW QUESTION 3
- (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 4
- (Topic 1)
Which of the following methods is the BEST way to demonstrate that an information security program provides appropriate coverage?

A. Security risk analysis
B. Gap assessment
C. Maturity assessment
D. Vulnerability scan report

Answer: B

Explanation:
A gap assessment is the best way to demonstrate that an information security program provides appropriate coverage, as it compares the current state of the information security program with the desired state based on the organization’s objectives, policies, standards, and regulations. A gap assessment can identify the strengths and weaknesses of the information security program, as well as the areas that need improvement or alignment. A gap assessment can also provide recommendations and action plans to close the gaps and achieve the desired level of information security coverage.
The other options are not as good as a gap assessment, as they do not provide a comprehensive and holistic view of the information security coverage. Security risk analysis is a process to identify and evaluate the risks to the information assets and the impact of potential threats and vulnerabilities. It can help to prioritize and mitigate the risks, but it does not measure the compliance or performance of the information security program. Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. It can help to validate and improve the technical security, but it does not assess the non-technical aspects of information security, such as governance, policies, or awareness. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234,
237-238.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1015.
? CISM domain 3: Information security program development and management [2022 update], Infosec Certifications, 2.

NEW QUESTION 5
- (Topic 1)
Which of the following is MOST effective in monitoring an organization's existing risk?

A. Periodic updates to risk register
B. Risk management dashboards
C. Security information and event management (SIEM) systems
D. Vulnerability assessment results

Answer: B

Explanation:
Risk management dashboards are the MOST effective in monitoring an organization’s existing risk because they provide a visual and interactive representation of the key risk indicators (KRIs) and metrics that reflect the current risk posture and performance of the organization. Risk management dashboards can help to communicate the risk information to various stakeholders, identify trends and patterns, compare actual results with targets and thresholds, and support decision making and risk response12. Periodic updates to risk register (A) are important to maintain the accuracy and relevance of the risk information, but they are not the most effective in monitoring the existing risk because they do not provide a real-time or dynamic view of the risk situation. Security information and event management (SIEM) systems © are effective in monitoring the security events and incidents that may indicate potential or actual threats to the organization, but they are not the most effective in monitoring the existing risk because they do not provide a comprehensive or holistic view of the risk context and impact. Vulnerability assessment results (D) are effective in monitoring the weaknesses and exposures of the organization’s assets and systems, but they are not the most effective in monitoring the existing risk because they do not provide a quantitative or qualitative measure of the risk likelihood and consequence. References = 1: CISM Review Manual 15th Edition, page 316-3171; 2: CISM Domain 2: Information Risk Management (IRM) [2022 update]2

NEW QUESTION 6
- (Topic 1)
Which of the following will result in the MOST accurate controls assessment?

A. Mature change management processes
B. Senior management support
C. Well-defined security policies
D. Unannounced testing

Answer: D

Explanation:
Unannounced testing is the most accurate way to assess the effectiveness of controls, as it simulates a real-world scenario and does not allow the staff to prepare or modify their behavior in advance. Mature change management processes, senior management support, and well-defined security policies are all important factors for establishing and maintaining a strong security posture, but they do not directly measure the performance of controls. References = CISM Review Manual, 16th Edition, page 149. CISM Questions, Answers & Explanations Database, question ID 1003.

NEW QUESTION 7
- (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 8
- (Topic 1)
Which of the following BEST ensures information security governance is aligned with corporate governance?

A. A security steering committee including IT representation
B. A consistent risk management approach
C. An information security risk register
D. Integration of security reporting into corporate reporting

Answer: D

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

NEW QUESTION 9
- (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 10
- (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 10
- (Topic 1)
Which of the following will BEST facilitate the integration of information security governance into enterprise governance?

A. Developing an information security policy based on risk assessments
B. Establishing an information security steering committee
C. Documenting the information security governance framework
D. Implementing an information security awareness program

Answer: B

Explanation:
Establishing an information security steering committee is the best way to facilitate the integration of information security governance into enterprise governance. The information security steering committee is a cross-functional group of senior managers who provide strategic direction, oversight, and support for the information security program. The committee ensures that the information security strategy is aligned with the enterprise strategy, objectives, and risk appetite. The committee also fosters collaboration and communication among various stakeholders and promotes a culture of security awareness and accountability. Developing an information security policy, documenting the information security governance framework, and implementing an information security awareness program are all important activities for implementing and maintaining information security governance, but they do not necessarily facilitate its integration into enterprise governance. These activities may be initiated or endorsed by the information security steering committee, but they are not sufficient to ensure that information security governance is embedded into the enterprise governance structure and
processes. References = CISM Review Manual 2023, page 34 1; CISM Practice Quiz 2

NEW QUESTION 14
- (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 17
- (Topic 1)
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.

Answer: D

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

NEW QUESTION 21
- (Topic 1)
When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

A. Data is encrypted in transit and at rest at the vendor site.
B. Data is subject to regular access log review.
C. The vendor must be able to amend data.
D. The vendor must agree to the organization's information security policy,

Answer: D

Explanation:
When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization’s information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization’s information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization’s right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

NEW QUESTION 23
- (Topic 1)
In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:

A. evaluate results of the most recent incident response test.
B. review the number of reported security incidents.
C. ensure established security metrics are reported.
D. assess progress of risk mitigation efforts.

Answer: D

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

NEW QUESTION 24
- (Topic 1)
Which of the following BEST ensures timely and reliable access to services?

A. Nonrepudiation
B. Authenticity
C. Availability
D. Recovery time objective (RTO)

Answer: C

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

NEW QUESTION 27
- (Topic 1)
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

A. The time and location that the breach occurred
B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error

Answer: C

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

NEW QUESTION 28
- (Topic 1)
Which of the following provides the BEST assurance that security policies are applied across business operations?

A. Organizational standards are included in awareness training.
B. Organizational standards are enforced by technical controls.
C. Organizational standards are required to be formally accepted.
D. Organizational standards are documented in operational procedures.

Answer: D

Explanation:
= The best assurance that security policies are applied across business operations is that organizational standards are documented in operational procedures. Operational procedures are the specific steps and actions that need to be taken to implement and comply with the security policies and standards. They provide clear and consistent guidance for the staff members who are responsible for performing the security tasks and functions. They also help to ensure that the security policies and standards are aligned with the business objectives and processes, and that they are measurable and auditable. Documenting the organizational standards in operational procedures can help to improve the security awareness, accountability, and performance of the staff members, and to reduce the risks of errors, deviations, and violations. The other options are not the best assurance because they are either too general or too specific. Organizational standards are included in awareness training (A) is a good practice to educate the staff members about the security policies and standards, but it does not guarantee that they will follow them or understand how to apply them in their daily operations. Organizational standards are enforced by technical controls (B) is a way to automate and monitor the compliance with the security policies and standards, but it does not cover all the aspects of security that may require human intervention or judgment. Organizational standards are required to be formally accepted © is a way to obtain the commitment and support from the staff members for the security policies and standards, but it does not ensure that they will adhere to them or know how to execute them in their work activities. References = CISM Review Manual 2022, pages 24-25, 28-29; CISM Item Development Guide 2022, page 9; Policies, Procedures, Standards, Baselines, and Guidelines | CISSP Security-Management Practices | Pearson IT Certification

NEW QUESTION 31
- (Topic 1)
In which cloud model does the cloud service buyer assume the MOST security responsibility?

A. Disaster Recovery as a Service (DRaaS)
B. Infrastructure as a Service (laaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)

Answer: B

Explanation:
Infrastructure as a Service (IaaS) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment.
In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page 140-1411

NEW QUESTION 36
- (Topic 1)
Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?

A. Establish key risk indicators (KRIs).
B. Use quantitative risk assessment methods.
C. Provide regular reporting on risk treatment to senior management
D. Require steering committee approval of risk treatment plans.

Answer: D

Explanation:
= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization’s risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization’s risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management. However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter 2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION 37
- (Topic 1)
Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

A. Documentation of control procedures
B. Standardization of compliance requirements
C. Automation of controls
D. Integration of assurance efforts

Answer: B

Explanation:
= Standardization of compliance requirements is the best approach to reduce unnecessary duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business partners. Standardization also facilitates the alignment of compliance activities with the organization’s risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. References = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

NEW QUESTION 38
- (Topic 1)
What should be the FIRST step when an Internet of Things (loT) device in an organization's network is confirmed to have been hacked?

A. Monitor the network.
B. Perform forensic analysis.
C. Disconnect the device from the network,
D. Escalate to the incident response team

Answer: C

Explanation:
= Disconnecting the device from the network is the first step when an IoT device in an organization’s network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures123. References =
? 1: CISM Review Manual 15th Edition, page 2004
? 2: CISM Practice Quiz, question 1072
? 3: IoT Security: Incident Response, Forensics, and Investigations, section “IoT Incident Response”

NEW QUESTION 43
- (Topic 1)
An organization is planning to outsource the execution of its disaster recovery activities. Which of the following would be MOST important to include in the outsourcing agreement?

A. Definition of when a disaster should be declared
B. Requirements for regularly testing backups
C. Recovery time objectives (RTOs)
D. The disaster recovery communication plan

Answer: C

Explanation:
The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on

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

NEW QUESTION 47
- (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 48
- (Topic 1)
IT projects have gone over budget with too many security controls being added post- production. Which of the following would MOST help to ensure that relevant controls are applied to a project?

A. Involving information security at each stage of project management
B. Identifying responsibilities during the project business case analysis
C. Creating a data classification framework and providing it to stakeholders
D. Providing stakeholders with minimum information security requirements

Answer: A

Explanation:
The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post- production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

NEW QUESTION 53
- (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 57
- (Topic 1)
Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

A. Evaluate privacy technologies required for data protection.
B. Encrypt all personal data stored on systems and networks.
C. Update disciplinary processes to address privacy violations.
D. Create an inventory of systems where personal data is stored.

Answer: D

Explanation:
= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:
? Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.
? Assess the risks and impacts associated with the personal data, and the compliance requirements and obligations under the applicable data privacy regulations.
? Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.
? Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.
? Monitor and review the performance and effectiveness of the data protection
program, and report and resolve any data breaches or incidents.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Data Protection, pages 202-2051; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 71, page 662.

NEW QUESTION 59
- (Topic 1)
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

A. Internal security audit
B. External security audit
C. Organizational risk appetite
D. Business impact analysis (BIA)

Answer: C

Explanation:
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

NEW QUESTION 60
- (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 63
- (Topic 1)
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?

A. Updated security policies
B. Defined security standards
C. Threat intelligence
D. Regular antivirus updates

Answer: C

Explanation:
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234,
237-238.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.
? Advanced Persistent Threats and Nation-State Actors 1
? Book Review: Advanced Persistent Threats 2
? Advanced Persistent Threat (APT) Protection 3
? Establishing Advanced Persistent Security to Combat Long-Term Threats 4
? What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION 64
- (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 69
- (Topic 1)
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.

Answer: D

Explanation:
The primary benefit of implementing a vulnerability assessment process is to facilitate proactive risk management. A vulnerability assessment process is a systematic and periodic evaluation of the security posture of an information system or network, which identifies and measures the weaknesses and exposures that may be exploited by threats. By implementing a vulnerability assessment process, the organization can proactively identify and prioritize the risks, and implement appropriate controls and mitigation strategies to reduce the likelihood and impact of potential incidents. The other options are possible benefits of implementing a vulnerability assessment process, but they are not the primary one. References = CISM Review Manual 15th Edition, page 1731; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1029

NEW QUESTION 72
- (Topic 1)
The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.

Answer: A

Explanation:
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources

are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION 75
- (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 78
- (Topic 1)
Which of the following is the BEST course of action for an information security manager to align security and business goals?

A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders

Answer: D

Explanation:
= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them. By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION 82
- (Topic 1)
The BEST way to identify the risk associated with a social engineering attack is to:

A. monitor the intrusion detection system (IDS),
B. review single sign-on (SSO) authentication lags.
C. test user knowledge of information security practices.
D. perform a business risk assessment of the email filtering system.

Answer: C

Explanation:
The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.
Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.

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

NEW QUESTION 86
- (Topic 1)
Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

A. Publish adopted information security standards.
B. Perform annual information security compliance reviews.
C. Implement an information security governance framework.
D. Define penalties for information security noncompliance.

Answer: C

Explanation:
The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

NEW QUESTION 90
- (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 92
- (Topic 1)
An organization finds it necessary to quickly shift to a work-fromhome model with an increased need for remote access security.
Which of the following should be given immediate focus?

A. Moving to a zero trust access model
B. Enabling network-level authentication
C. Enhancing cyber response capability
D. Strengthening endpoint security

Answer: D

Explanation:
Strengthening endpoint security is the most immediate focus when shifting to a work-from- home model with an increased need for remote access security, as this reduces the risk of unauthorized access, data leakage, malware infection, and other threats that may compromise the confidentiality, integrity, and availability of the organization's information assets. Moving to a zero trust access model, enabling network-level authentication, and enhancing cyber response capability are also important, but not as urgent as strengthening endpoint security, as they require more time, resources, and planning to implement effectively. References = CISM Review Manual 2023, page 1561; CISM Review Questions, Answers & Explanations Manual 2023, page 302; ISACA CISM - iSecPrep, page 153

NEW QUESTION 93
- (Topic 3)
Which of the following should include contact information for representatives of equipment and software vendors?

A. Information security program charter
B. Business impact analysis (BIA)
C. Service level agreements (SLAs)
D. Business continuity plan (BCP)

Answer: D

Explanation:
The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization’s critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/business-continuity- management-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

NEW QUESTION 95
- (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 98
- (Topic 3)
Which of the following metrics is MOST appropriate for evaluating the incident notification process?

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

Answer: D

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

NEW QUESTION 99
- (Topic 3)
Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?

A. Demonstrating the program's value to the organization
B. Discussing governance programs found in similar organizations
C. Providing the results of external audits
D. Providing examples of information security incidents within the organization

Answer: A

Explanation:
The best way to obtain senior management support for an information security governance program is to demonstrate the program’s value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. References:
? https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process

? https://www.sans.org/white-papers/992/
? https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for-your-security-program.html

NEW QUESTION 102
- (Topic 3)
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?

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

Answer: D

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

NEW QUESTION 104
- (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 108
- (Topic 3)
Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?

A. Conducting periodic vulnerability assessments
B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework

Answer: C

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

NEW QUESTION 113

- (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 114
- (Topic 3)
Which of the following should be the FIRST step when performing triage of a malware incident?

A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware

Answer: A

Explanation:
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION 118
- (Topic 3)
The PRIMARY consideration when responding to a ransomware attack should be to ensure:

A. backups are available.
B. the most recent patches have been applied.
C. the ransomware attack is contained
D. the business can operate

Answer: D

Explanation:
Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
? https://www.cisa.gov/stopransomware/ransomware-guide
? https://csrc.nist.gov/Projects/ransomware-protection-and-response
? https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect- respond

NEW QUESTION 119
- (Topic 3)
Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

A. Escalation processes
B. Recovery time objective (RTO)
C. Security audit reports
D. Technological capabilities

Answer: A

Explanation:
Escalation processes are the most important security consideration when developing an incident response strategy with a cloud provider, as they define the roles, responsibilities, communication channels, and decision-making authority for both parties in the event of a security incident. Escalation processes help to ensure timely and effective response, coordination, and resolution of security incidents, as well as to avoid conflicts or confusion. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION 124
- (Topic 1)
Which of the following is MOST important in increasing the effectiveness of incident responders?

A. Communicating with the management team
B. Integrating staff with the IT department
C. Testing response scenarios
D. Reviewing the incident response plan annually

Answer: C

Explanation:
= Testing response scenarios is the most important factor in increasing the
effectiveness of incident responders, as it allows them to practice their skills, identify gaps and weaknesses, evaluate the adequacy and feasibility of the incident response plan, and improve their coordination and communication. Testing response scenarios can also help to enhance the confidence and readiness of the incident responders, as well as to measure their performance and compliance with the policies and procedures. Testing response scenarios can be done through various methods, such as tabletop exercises, simulations, drills, or full-scale exercises, depending on the scope, objectives, and complexity of the scenarios.
The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents. However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

NEW QUESTION 128
- (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 129
- (Topic 3)
Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?

A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.
D. Provide security awareness training to board executives.

Answer: A

Explanation:
The best way to help ensure alignment of the information security program with organizational objectives is A. Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by:
Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators
Allocating and prioritizing the resources and budget for information security initiatives and projects
Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security
An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

NEW QUESTION 130
- (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 135
- (Topic 3)
Which of the following is the BEST way to ensure the business continuity plan (BCP) is current?

A. Manage business process changes.
B. Update business impact analyses (BIAs) on a regular basis.
C. Conduct periodic testing.
D. Review and update emergency contact lists.

Answer: C

Explanation:
Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.
References: The CISM Review Manual 2023 states that "testing is a critical component of the BCP process" and that "testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations" (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this Answer "Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update" (p. 98). Additionally, the article Business Continuity Planning:
Testing an Organization's Plan from the ISACA Journal 2019 states that "testing is essential to ensure that the BCP is current and effective" and that "testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks" (p. 1)

NEW QUESTION 137
- (Topic 3)
An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?

A. Implementing automated vulnerability scanning in the help desk workflow
B. Changing the default setting for all security incidents to the highest priority
C. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system
D. Integrating incident response workflow into the help desk ticketing system

Answer: D

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

NEW QUESTION 142
- (Topic 3)
Which of the following is the MOST effective way to ensure information security policies are understood?

A. Implement a whistle-blower program.
B. Provide regular security awareness training.
C. Include security responsibilities in job descriptions.
D. Document security procedures.

Answer: B

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

NEW QUESTION 145
- (Topic 3)
Which of the following MUST be established to maintain an effective information security governance framework?

A. Security controls automation
B. Defined security metrics
C. Change management processes
D. Security policy provisions

Answer: D

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

NEW QUESTION 148
- (Topic 3)
Which of the following is the GREATEST challenge with assessing emerging risk in an organization?

A. Lack of a risk framework
B. Ineffective security controls
C. Presence of known vulnerabilities
D. Incomplete identification of threats

Answer: D

Explanation:
The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed. Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment. References:
? https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.html
? https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging-risk-analysis
? https://projectriskcoach.com/emerging-risks/

NEW QUESTION 149
- (Topic 3)
Which of the following is MOST important to have in place for an organization's information security program to be effective?

A. Documented information security processes
B. A comprehensive IT strategy
C. Senior management support
D. Defined and allocated budget

Answer: C

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

NEW QUESTION 150
- (Topic 3)
An information security manager wants to document requirements detailing the minimum security controls required for user workstations. Which of the following resources would be MOST appropriate for this purposed?

A. Guidelines
B. Policies
C. Procedures
D. Standards

Answer: D

Explanation:
Standards are detailed statements of the minimum requirements for hardware, software, or security configurations. They are used to define the minimum security controls required for user workstations. References = CISM Review Manual, 16th Edition, page 69.

NEW QUESTION 151
- (Topic 3)
An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.

D. Determine compensating controls.

Answer: C

Explanation:
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third-party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION 154
- (Topic 3)
Which of the following is the BEST way to determine the effectiveness of an incident response plan?

A. Reviewing previous audit reports
B. Conducting a tabletop exercise
C. Benchmarking the plan against best practices
D. Performing a penetration test

Answer: B

Explanation:
A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

NEW QUESTION 159
- (Topic 2)
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

A. Monitor the effectiveness of controls
B. Update the risk assessment framework
C. Review the inherent risk level
D. Review the risk probability and impact

Answer: A

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

NEW QUESTION 161
- (Topic 2)
To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls

Answer: B

Explanation:
To support effective risk decision making, it is most important to have risk reporting procedures in place. Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization’s structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid-level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION 164
- (Topic 2)
An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

A. Establishing the authority to remote wipe
B. Developing security awareness training
C. Requiring the backup of the organization's data by the user
D. Monitoring how often the smartphone is used

Answer: A

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

NEW QUESTION 167
- (Topic 2)
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process

Answer: D

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

NEW QUESTION 170
- (Topic 2)
Which of the following would be MOST effective in gaining senior management approval of security investments in network infrastructure?

A. Performing penetration tests against the network to demonstrate business vulnerability
B. Highlighting competitor performance regarding network best security practices
C. Demonstrating that targeted security controls tie to business objectives
D. Presenting comparable security implementation estimates from several vendors

Answer: C

Explanation:
The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives.

Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.

According to the Certified Information Security Manager (CISM) Study Manual, "To gain senior management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization."

While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.

Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

NEW QUESTION 175
- (Topic 2)
An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?

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

Answer: B

Explanation:
Isolating the endpoint device is the best course of action to prevent further damage, as it will prevent the potential spread of malware or compromise to other devices or systems on the network. Wiping and resetting the endpoint device may be a possible recovery option, but it is not the first priority and it may also destroy valuable forensic evidence. Powering off the endpoint device may also cause loss of data or evidence, and it may not stop the attack if the device is remotely controlled. Running a virus scan on the endpoint device may not be effective if the device is already compromised, and it may also trigger malicious actions by the attacker. References = CISM Review Manual 15th Edition, page 203. Boosting Cyberresilience for Critical Enterprise IT Systems With COBIT and NIST Cybersecurity Frameworks1, Endpoint Security: On the Frontline of Cyber Risk2.
The best course of action to prevent further damage is to isolate the endpoint device. Isolating the endpoint device will prevent the compromised system from connecting to other systems on the network and spreading the infection. Other possible courses of action include wiping and resetting the endpoint device, running a virus scan, and powering off the endpoint device. However, these actions will not prevent the compromised system from continuing to spread the infection.

NEW QUESTION 178
- (Topic 2)
Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

A. Risk acceptance by the business has been documented
B. Teams and individuals responsible for recovery have been identified
C. Copies of recovery and incident response plans are kept offsite
D. Incident response and recovery plans are documented in simple language

Answer: B

Explanation:
Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities. This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

NEW QUESTION 182
- (Topic 2)
The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.

Answer: D

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

NEW QUESTION 183
......