Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
- (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 2
- (Topic 1)
Which of the following will have the GREATEST influence on the successful adoption of an information security governance program?

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

Answer: D

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

NEW QUESTION 3
- (Topic 1)
Penetration testing is MOST appropriate when a:

A. new system is about to go live.
B. new system is being designed.
C. security policy is being developed.
D. security incident has occurred,

Answer: A

Explanation:
= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

NEW QUESTION 4
- (Topic 1)
Which of the following BEST indicates that information assets are classified accurately?

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

Answer: A

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

NEW QUESTION 5
- (Topic 1)
Which of the following BEST facilitates effective incident response testing?

A. Including all business units in testing
B. Simulating realistic test scenarios
C. Reviewing test results quarterly
D. Testing after major business changes

Answer: B

Explanation:
Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective testing is to simulate realistic test scenarios that reflect the most likely or critical threats and vulnerabilities that could cause an incident, and the most relevant or significant impacts and consequences that could result from an incident. Simulating realistic test scenarios can help to evaluate the adequacy, accuracy, and applicability of the incident response plan, procedures, roles, and resources, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the incident response process. Simulating realistic test scenarios can also help to enhance the skills, knowledge, and experience of the incident response team and the organization, as well as to improve the communication, coordination, and collaboration among the stakeholders involved in the incident response process. Simulating realistic test scenarios
can also help to measure and report the effectiveness and efficiency of the incident response process, and to provide feedback and recommendations for improvement and optimization. References = CISM Review Manual 15th Edition, page 2401; CISM Practice Quiz, question 1362

NEW QUESTION 6
- (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 7
- (Topic 1)
Which of the following BEST supports information security management in the event of organizational changes in security personnel?

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

Answer: C

Explanation:
Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION 8
- (Topic 1)
Which of the following would be the BEST way for an information security manager to improve the effectiveness of an organization's information security program?

A. Focus on addressing conflicts between security and performance.
B. Collaborate with business and IT functions in determining controls.
C. Include information security requirements in the change control process.
D. Obtain assistance from IT to implement automated security cantrals.

Answer: B

Explanation:
The best way for an information security manager to improve the effectiveness of an organization's information security program is to collaborate with business and IT functions in determining controls. Collaboration is a key factor for ensuring that the information security program is aligned with the organization's business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program. Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions.
Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance, and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.
Including information security requirements in the change control process © is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.
Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy Development, Subsection: Collaboration, page 24-251

NEW QUESTION 9
- (Topic 1)
Which of the following is the PRIMARY role of an information security manager in a software development project?

A. To enhance awareness for secure software design
B. To assess and approve the security application architecture
C. To identify noncompliance in the early design stage
D. To identify software security weaknesses

Answer: B

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

NEW QUESTION 10
- (Topic 1)
An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.

Answer: C

Explanation:
A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:
? It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.
? It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
? It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
? It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
? It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.
The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. References = 1: What is a Gap Analysis? |
Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:
* 1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

NEW QUESTION 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 15
- (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 18
- (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 20
- (Topic 1)
The MOST appropriate time to conduct a disaster recovery test would be after:

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

Answer: B

Explanation:
The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well
as identify any gaps, issues, or improvement opportunities123. References =
? 1: CISM Review Manual 15th Edition, page 2114
? 2: CISM Practice Quiz, question 1042
? 3: Business Continuity Planning and Disaster Recovery Testing, section "Testing the Plan"

NEW QUESTION 21
- (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 24
- (Topic 1)
During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

A. Post-incident review
B. Eradication
C. Containment
D. Identification

Answer: B

Explanation:
The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2.
The other phases of incident response are:
? Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
? Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
? Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.
? Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.

? Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2: What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

NEW QUESTION 28
- (Topic 1)
An organization is close to going live with the implementation of a cloud-based application. Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?

A. Implement the application and request the cloud service provider to fix the vulnerability.
B. Assess whether the vulnerability is within the organization's risk tolerance levels.
C. Commission further penetration tests to validate initial test results,
D. Postpone the implementation until the vulnerability has been fixed.

Answer: B

Explanation:
The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization’s risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.
Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.
Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information. The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project. Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization’s reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk- averse approach, as it may hinder the organization’s innovation and competitiveness. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

NEW QUESTION 29
- (Topic 1)
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

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

Answer: B

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

NEW QUESTION 34
- (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 37
- (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 41
- (Topic 1)
An information security manager developing an incident response plan MUST ensure it includes:

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

Answer: B

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

NEW QUESTION 42
- (Topic 1)
An online bank identifies a successful network attack in progress. The bank should FIRST:

A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (Pll) is compromised.
D. shut down the entire network.

Answer: A

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

NEW QUESTION 44
- (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 49
- (Topic 1)
An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?

A. Enforce the policy.
B. Modify the policy.
C. Present the risk to senior management.
D. Create an exception for the deviation.

Answer: C

Explanation:
The information security manager’s best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role-based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management’s approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127- 128, 138-139, 143-144.

NEW QUESTION 52
- (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 54
- (Topic 1)
Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards

Answer: C

Explanation:
= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information

security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION 56
- (Topic 1)
Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage
B. Communicating with internal and external parties
C. Minimizing negative impact to critical operations
D. Classifying incidents

Answer: C

Explanation:
The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents. The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.
Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed. However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION 57
- (Topic 1)
When deciding to move to a cloud-based model, the FIRST consideration should be:

A. storage in a shared environment.
B. availability of the data.
C. data classification.
D. physical location of the data.

Answer: C

Explanation:
The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.
Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co-located with other customers' data, and may be subject to unauthorized access, modification, or deletion. Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies. However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

NEW QUESTION 58
- (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 60
- (Topic 1)
Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.

Answer: B

Explanation:
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
? 1: Information Security Incident Response Escalation Guideline2, page 4
? 2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
? 3: Computer Security Incident Handling Guide4, page 18

NEW QUESTION 63
- (Topic 1)
Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

A. To compare emerging trends with the existing organizational security posture
B. To communicate worst-case scenarios to senior management
C. To train information security professionals to mitigate new threats
D. To determine opportunities for expanding organizational information security

Answer: A

Explanation:
The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce
the likelihood and impact of cyberattacks. References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

NEW QUESTION 66
- (Topic 1)
Which of the following is a desired outcome of information security governance?

A. Penetration test
B. Improved risk management
C. Business agility
D. A maturity model

Answer: C

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

NEW QUESTION 68
- (Topic 3)
When developing a categorization method for security incidents, the categories MUST:

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

Answer: C

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

NEW QUESTION 72
- (Topic 3)
Which of the following BEST indicates that an information security governance framework has been successfully implemented?

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

Answer: A

Explanation:
The best indicator that an information security governance framework has been successfully implemented is A. The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.
The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

NEW QUESTION 75
- (Topic 3)
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

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

Answer: A

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

NEW QUESTION 77
- (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 80
- (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 82
- (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 86
- (Topic 3)
Which of the following is the MOST effective way to identify changes in an information security environment?

A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring

Answer: D

Explanation:
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security

status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371)
References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

NEW QUESTION 90
- (Topic 3)
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

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

Answer: B

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

NEW QUESTION 94
- (Topic 3)
When establishing an information security governance framework, it is MOST important for an information security manager to understand:

A. information security best practices.
B. risk management techniques.
C. the threat environment.
D. the corporate culture.

Answer: D

NEW QUESTION 99
- (Topic 1)
An information security manager is reporting on open items from the risk register to senior management. Which of the following is MOST important to communicate with regard to these risks?

A. Responsible entities
B. Key risk indicators (KRIS)
C. Compensating controls
D. Potential business impact

Answer: D

Explanation:
The most important information to communicate with regard to the open items from the risk register to senior management is the potential business impact of these risks. The potential business impact is the estimated consequence or loss that the organization may suffer if the risk materializes or occurs. The potential business impact can be expressed in quantitative or qualitative terms, such as financial, operational, reputational, legal, or strategic impact. Communicating the potential business impact of the open items from the risk register helps senior management to understand the severity and urgency of these risks, and to prioritize the risk response actions and resources accordingly. Communicating the potential business impact also helps senior management to align the risk management objectives and activities with the business objectives and strategies, and to ensure that the risk appetite and tolerance of the organization are respected and maintained.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk
Management, Section: Risk Assessment, page 831; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Reporting, page 1012.

NEW QUESTION 102
- (Topic 1)
In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:

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

Answer: B

Explanation:
= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities,

impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management. References =
? CISM Review Manual 15th Edition, page 1131
? CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482
? CISM Domain 2: Information Risk Management (IRM) [2022 update]3

NEW QUESTION 105
- (Topic 3)
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?

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

Answer: C

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

NEW QUESTION 110
- (Topic 3)
Which of the following is MOST important to maintain integration among the incident response plan, business continuity plan (BCP). and disaster recovery plan (DRP)?

A. Asset classification
B. Recovery time objectives (RTOs)
C. Chain of custody
D. Escalation procedures

Answer: B

Explanation:
Recovery time objectives (RTOs) are the maximum acceptable time that an organization can be offline or unavailable after a disruption. RTOs are important to maintain integration among the incident response plan, business continuity plan (BCP), and disaster recovery plan (DRP) because they help align the recovery goals and strategies of each plan. By defining clear and realistic RTOs, an organization can ensure that its IT infrastructure and systems are restored as quickly as possible after a disaster, minimizing the impact on business operations and customer satisfaction.
References = CISM Manual, Chapter 6: Incident Response Planning, Section 6.2: Recovery Time Objectives (RTOs), page 971
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION 111
- (Topic 3)
Senior management has just accepted the risk of noncompliance with a new regulation What should the information security manager do NEX*P

A. Report the decision to the compliance officer
B. Update details within the risk register.
C. Reassess the organization's risk tolerance.
D. Assess the impact of the regulation.

Answer: B

Explanation:
Updating details within the risk register is the next step for the information security manager to do after senior management has accepted the risk of noncompliance with a new regulation because it records and communicates the risk status, impact, and response strategy to the relevant stakeholders. Reporting the decision to the compliance officer is not the next step, but rather a possible subsequent step that involves informing and consulting with the compliance officer about the risk acceptance and its implications. Reassessing the organization’s risk tolerance is not the next step, but rather a possible subsequent step that involves reviewing and adjusting the organization’s risk appetite and thresholds based on the risk acceptance and its implications. Assessing the impact of the regulation is not the next step, but rather a previous step that involves analyzing and evaluating the potential consequences and likelihood of noncompliance with the regulation. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

NEW QUESTION 115
- (Topic 3)
Which of the following should be triggered FIRST when unknown malware has infected an organization's critical system?

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

Answer: A

Explanation:
The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization's critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response- lessons-learned

NEW QUESTION 120
- (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 121
- (Topic 3)
A newly appointed information security manager has been asked to update all security- related policies and procedures that have been static for five years or more. What should be done NEXT?

A. Update in accordance with the best business practices.
B. Perform a risk assessment of the current IT environment.
C. Gain an understanding of the current business direction.
D. Inventory and review current security policies.

Answer: D

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

NEW QUESTION 126
- (Topic 3)
The categorization of incidents is MOST important for evaluating which of the following?

A. Appropriate communication channels
B. Allocation of needed resources
C. Risk severity and incident priority
D. Response and containment requirements

Answer: C

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

NEW QUESTION 128
- (Topic 3)
Which of the following is MOST important to include in an information security status report management?

A. List of recent security events
B. Key risk indication (KRIs)
C. Review of information security policies
D. information security budget requests

Answer: B

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

NEW QUESTION 129
- (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 132
- (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 135
- (Topic 3)
Which of the following is ESSENTIAL to ensuring effective incident response?

A. Business continuity plan (BCP)
B. Cost-benefit analysis
C. Classification scheme
D. Senior management support

Answer: D

Explanation:
Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.
The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality. References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

NEW QUESTION 136

- (Topic 2)
An information security manager believes that information has been classified inappropriately, = the risk of a breach. Which of the following is the information security manager's BEST action?

A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.
D. Complete a risk assessment and refer the results to the data owners.

Answer: D

Explanation:
= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.
If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach, as well as the cost and benefit of implementing additional security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.
The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security manager. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

NEW QUESTION 141
- (Topic 2)
Which of the following has the GREATEST influence on an organization's information security strategy?

A. The organization's risk tolerance
B. The organizational structure
C. Industry security standards
D. Information security awareness

Answer: A

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

NEW QUESTION 146
- (Topic 2)
Which of the following is the BEST approach when creating a security policy for a global organization subject to varying laws and regulations?

A. Incorporate policy statements derived from third-party standards and benchmarks.
B. Adhere to a unique corporate privacy and security standard
C. Establish baseline standards for all locations and add supplemental standards as required
D. Require that all locations comply with a generally accepted set of industry

Answer: C

Explanation:
= Creating a security policy for a global organization subject to varying laws and regulations is a challenging task, as it requires balancing the need for consistency, compliance, and flexibility. The best approach is to establish baseline standards for all locations that reflect the organization’s overall security objectives, principles, and requirements. These standards should be aligned with the organization’s mission, vision, values, and strategy, as well as with the applicable laws and regulations of each location. The baseline standards should also be reviewed and updated periodically to ensure their relevance and effectiveness. Additionally, supplemental standards can be added as required to address specific issues or risks that may arise in different locations or situations. Supplemental standards should be based on the best practices and lessons learned from the baseline standards, as well as on the feedback and input from the stakeholders of each location. References = CISM Review Manual, 16th Edition, page 1001

NEW QUESTION 149
- (Topic 2)
Which of the following desired outcomes BEST supports a decision to invest in a new security initiative?

A. Enhanced security monitoring and reporting
B. Reduced control complexity
C. Enhanced threat detection capability
D. Reduction of organizational risk

Answer: D

Explanation:
The reduction of organizational risk is the desired outcome that best supports a decision to invest in a new security initiative. The organizational risk is the level of exposure or uncertainty that the organization faces in achieving its objectives. The organizational risk is influenced by various factors, such as the threat landscape, the vulnerability of the assets, the impact of the incidents, and the effectiveness of the controls. The information security manager should evaluate the organizational risk and propose security initiatives that can reduce the risk to an acceptable level. The security initiatives should be aligned with the business goals, the risk appetite, and the available resources of the organization. The security initiatives should also provide a positive return on investment (ROI) or value for money (VFM) for the organization. The reduction of organizational risk is the ultimate goal and benefit of any security initiative, as it enhances the security posture, performance, and resilience of the organization. Enhanced security monitoring and reporting, reduced control complexity, and enhanced threat detection capability are all possible outcomes of security initiatives, but they are not the best ones to support a decision to invest in a new security initiative. These outcomes are more specific and technical, and they may not directly relate to the business objectives or the risk appetite of the organization. These outcomes are also intermediate or enabling, rather than final or ultimate, as they may not necessarily lead to the reduction of organizational risk. For example, enhanced security monitoring and reporting may improve the visibility and awareness of the security status, but it may not prevent or mitigate the incidents. Reduced control complexity may simplify the security management and maintenance, but it may not address the emerging or evolving threats. Enhanced threat detection capability may increase the speed and accuracy of identifying the attacks, but it may not reduce the impact or the likelihood of the attacks. Therefore, the reduction of organizational risk is the best outcome to support a decision to invest in a new security initiative, as it demonstrates the value and effectiveness of the security initiative for the organization.
References = CISM Review Manual 2023, page 40 1; CISM Practice Quiz 2

NEW QUESTION 154
- (Topic 2)
Which of the following is MOST helpful for aligning security operations with the IT governance framework?

A. Security risk assessment
B. Security operations program
C. Information security policy
D. Business impact analysis (BIA)

Answer: C

Explanation:
An information security policy is the MOST helpful for aligning security operations with the IT governance framework because it defines the security objectives, principles, standards, and guidelines that guide the security operations activities and processes. An information security policy also establishes the roles and responsibilities, authorities and accountabilities, and reporting and communication mechanisms for security operations. An information security policy should be aligned with the IT governance framework, which provides the direction, structure, and oversight for the effective management and delivery of IT services and resources. An information security policy should also be consistent with the enterprise governance framework, which sets the vision, mission, values, and goals of the organization12. A security risk assessment (A) is helpful for identifying and evaluating the security risks that may affect the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A security risk assessment should be based on the information security policy, which defines the risk appetite, tolerance, and criteria for the organization12. A security operations program (B) is helpful for implementing and executing the security operations activities and processes that support the IT governance framework, but it is not the MOST helpful for aligning them. A security operations program should be derived from the information security policy, which provides the strategic direction and guidance for the security operations12. A business impact analysis (BIA) (D) is helpful for determining the criticality and priority of the business processes and functions that depend on the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A BIA should be conducted in accordance with the information security policy, which specifies the business continuity and disaster recovery requirements and objectives for the organization12. References = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG) [2022 update]2

NEW QUESTION 158
- (Topic 2)
Which of the following is the MOST effective way to prevent information security incidents?

A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment

Answer: B

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

NEW QUESTION 161
- (Topic 2)
Labeling information according to its security classification:

A. enhances the likelihood of people handling information securely.
B. reduces the number and type of countermeasures required.

C. reduces the need to identify baseline controls for each classification.
D. affects the consequences if information is handled insecurely.

Answer: A

Explanation:
Labeling information according to its security classification enhances the likelihood of people handling information securely. Security classification is a process of categoriz-ing information based on its level of sensitivity and importance, and applying appropri-ate security controls based on the level of risk associated with that infor-mation1. Labeling is a process of marking the information with the appropriate classifi-cation level, such as public, internal, confidential, secret, or top secret2. The purpose of labeling is to inform the users of the information about its value and protection re-quirements, and to guide them on how to handle it securely. Labeling can help users to:
•Identify the information they are dealing with and its classification level
•Understand their roles and responsibilities regarding the information
•Follow the security policies and procedures for the information
•Avoid unauthorized access, disclosure, modification, or destruction of the information
•Report any security incidents or breaches involving the information Labeling can also help organizations to:
•Track and monitor the information and its usage
•Enforce access controls and encryption for the information
•Audit and review the compliance with security standards and regulations for the infor- mation
•Educate and train employees and stakeholders on information security awareness and best practices
Therefore, labeling information according to its security classification enhances the likelihood of people handling information securely, as it increases their awareness and accountability, and supports the implementation of security measures. The other op-tions are not the primary benefits of labeling information according to its security clas-sification. Reducing the number and type of countermeasures required is not a benefit, but rather a consequence of applying security controls based on the classification lev-el. Reducing the need to identify baseline controls for each classification is not a bene-fit, but rather a prerequisite for labeling information according to its security classifica-tion. Affecting the consequences if information is handled insecurely is not a benefit, but rather a risk that needs to be managed by implementing appropriate security con-trols and incident response procedures. References: 1: Information Classification - Ad-visera 2: Information Classification in Information Security - GeeksforGeeks : Infor-mation Security Policy - NIST : Information Security Classification Framework - Queensland Government

NEW QUESTION 165
- (Topic 2)
When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?

A. Business process owner
B. Business continuity coordinator
C. Senior management
D. Information security manager

Answer: A

Explanation:
The business process owner is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization’s operations and objectives. The business process owner has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the business process owner is the best person to calculate the recovery time and cost estimates when performing a business impact analysis (BIA), which is a process of identifying and quantifying the potential losses, damages, or consequences that could result from a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The recovery time and cost estimates are the measures that indicate the time and money that are needed to resume and restore the normal business operations and functions after the disruption or incident. The recovery time and cost estimates can help to prioritize and protect the critical activities and resources, to allocate the appropriate budget and resources, to implement the necessary controls and measures, and to evaluate the effectiveness and efficiency of the business continuity and disaster recovery plans.
The business continuity coordinator, the senior management, and the information security manager are all important roles in the BIA process, but they are not the best ones to calculate the recovery time and cost estimates. The business continuity coordinator is the person who is responsible for coordinating and facilitating the BIA process, as well as the development, implementation, and maintenance of the business continuity and disaster recovery plans. The business continuity coordinator can help to define and communicate the scope, objectives, and methodology of the BIA, to collect and analyze the data and information from the business process owners and other stakeholders, to report and present the BIA results and recommendations, and to provide feedback and suggestions for improvement and optimization of the BIA and the plans. The senior management is the group of people who have the ultimate authority and accountability for the organization’s strategy, direction, and performance. The senior management can help to approve and support the BIA process and the plans, to provide the strategic guidance and vision for the business continuity and disaster recovery, to allocate the necessary budget and resources, to oversee and monitor the BIA and the plans, and to make the final decisions and approvals. The information security manager is the person who is responsible for ensuring the security of the information assets and systems that support the business processes and functions. The information security manager can help to identify and assess the information security risks and issues that could affect the BIA and the plans, to implement and manage the security controls and measures that are needed to protect and recover the information assets and systems, to coordinate and collaborate with the business process owners and other stakeholders on the security aspects of the BIA and the plans, and to provide the security expertise and advice. References = CISM Review Manual 15th Edition, pages 228-2291; CISM Practice Quiz, question 1722

NEW QUESTION 167
- (Topic 2)
Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Require remote wipe capabilities for devices.
B. Conduct security awareness training.
C. Review and update existing security policies.
D. Enforce passwords and data encryption on the devices.

Answer: C

Explanation:
The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation’s security program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be reviewed and updated regularly to reflect

changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities, as well as new opportunities and benefits, for the organiza- tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:
•The scope, purpose, and ownership of company-owned mobile devices
•The acceptable and unacceptable use of company-owned mobile devices
•The security standards and best practices for company-owned mobile devices
•The roles and responsibilities of users, managers, IT staff, and vendors regarding compa- ny-owned mobile devices
•The procedures for provisioning, managing, monitoring, and decommissioning company- owned mobile devices
•The incident response and reporting process for company-owned mobile devices
By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com-promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices. References: 1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is & How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

NEW QUESTION 171
- (Topic 2)
Which of the following BEST enables the integration of information security governance into corporate governance?

A. Well-decumented information security policies and standards
B. An information security steering committee with business representation
C. Clear lines of authority across the organization
D. Senior management approval of the information security strategy

Answer: B

Explanation:
= The best way to enable the integration of information security governance into corporate governance is to establish an information security steering committee with business representation. An information security steering committee is a group of senior executives and managers from different business units and functions who are responsible for overseeing, directing, and supporting the information security program and strategy of the organization. An information security steering committee with business representation can enable the integration of information security governance into corporate governance by providing the following benefits12:
? Align the information security objectives and priorities with the business objectives and priorities, and ensure that the information security program and strategy support and enable the achievement of the organizational goals and performance.
? Communicate and promote the value and importance of information security to the board of directors, senior management, and other stakeholders, and ensure that information security is considered and incorporated in the decision making and planning processes of the organization.
? Provide guidance and direction to the information security manager and the information security team, and ensure that they have the necessary authority, resources, and support to implement and maintain the information security program and strategy effectively and efficiently.
? Monitor and evaluate the performance and outcomes of the information security program and strategy, and ensure that they are aligned with the expectations and requirements of the organization and its stakeholders, as well as the relevant laws, regulations, standards, and best practices.
? Identify and address the issues, challenges, and opportunities related to information security, and ensure that the information security program and strategy are continuously improved and updated to reflect the changes and developments in the internal and external environment.
The other options are not the best way to enable the integration of information security governance into corporate governance, as they are less comprehensive, effective, or influential than establishing an information security steering committee with business representation. Well-documented information security policies and standards are important components of the information security program and strategy, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not reflect or align with the business needs, priorities, or expectations, and they may not be communicated, implemented, or enforced properly or consistently across the organization. Clear lines of authority across the organization are important factors for the information security governance structure, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not ensure the involvement, participation, or support of the senior executives, managers, and other stakeholders who are responsible for or affected by information security. Senior management approval of the information security strategy is an important outcome of the information security governance process, but it is not sufficient to enable the integration of information security governance into corporate governance, as it may not ensure the alignment, communication, or monitoring of the information security strategy with the business strategy, and it may not ensure the accountability, responsibility, or authority of the information security manager and the information security team12. References = CISM Domain 1: Information Security Governance (ISG) [2022 update], Information Security Governance for CISM® | Pluralsight, Aligning Information Security with Business Strategy - ISACA, Aligning Information Security with Business Objectives - ISACA

NEW QUESTION 175
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISM Practice Exam Features:

* CISM Questions and Answers Updated Frequently

* CISM Practice Questions Verified by Expert Senior Certified Staff

* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year