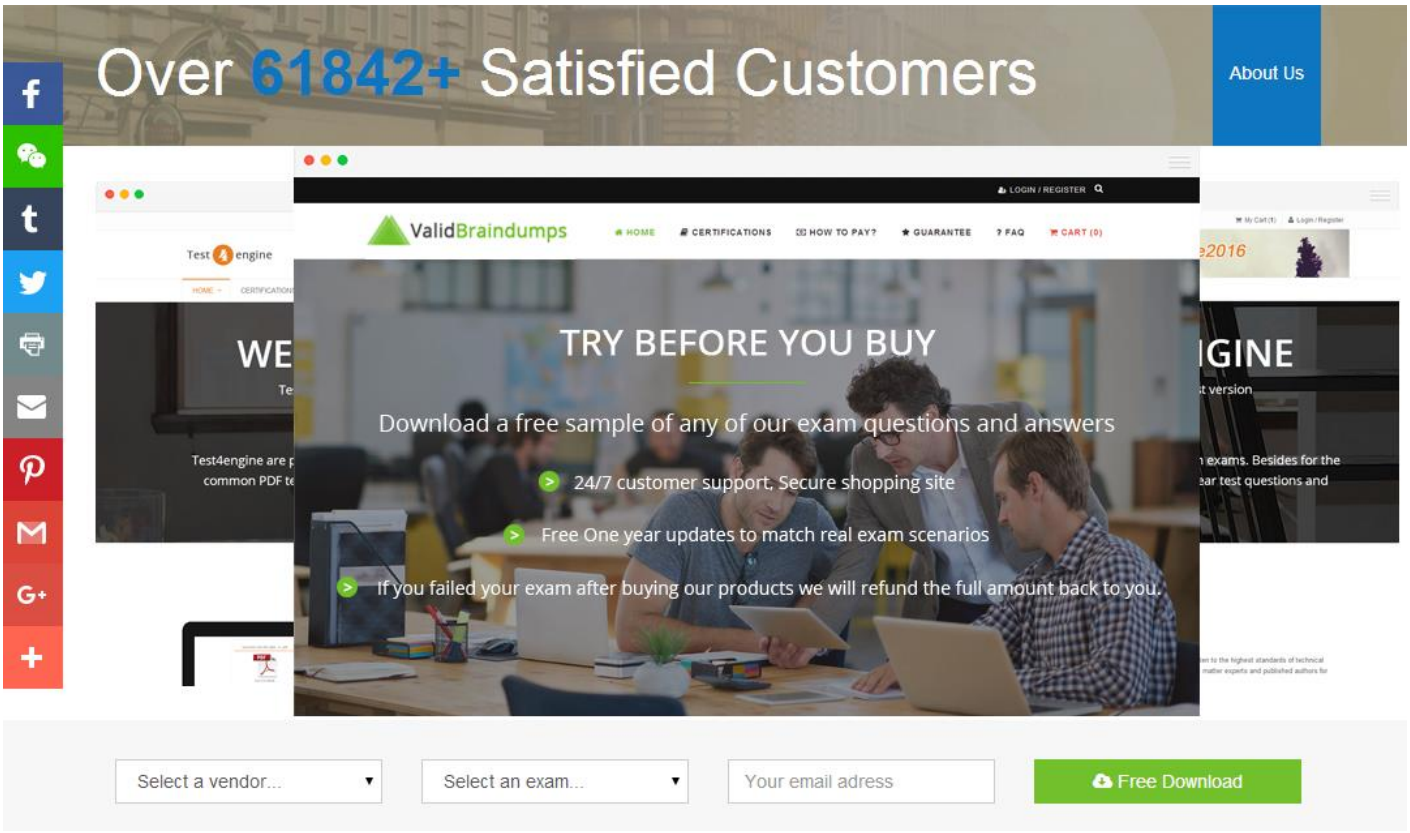
ValidBraindumps



Try Before You Buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

http://www.validbraindumps.com

Free valid test braindumps for IT certification valid exam

Exam : **CISM**

Title : Certified Information Security Manager

Vendor : ISACA

Version : DEMO

NO.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

NO.2 Who is accountable for ensuring proper controls are in place to address the confidentiality and availability of an information system?

A. Senior management

B. Information owner

C. Business manager

D. Information security manager

Answer: A

NO.3 Which of the following should an organization do FIRST when confronted with the transfer of personal data across borders?

A. Define policies and standards for data processing.

B. Implement applicable privacy principles

C. Assess local or regional regulations

D. Research cyber insurance policies

Answer: C

Explanation:

Before transferring personal data across borders, an organization should first assess the local or regional regulations that apply to the data protection and privacy of the data subjects. This will help the organization to identify the legal requirements and risks involved in the data transfer, and to choose the appropriate tools and safeguards to ensure compliance and protection. For example, the organization may need to obtain consent from the data subjects, use adequacy decisions, standard contractual clauses, or other mechanisms to ensure an adequate level of protection in the third country, or rely on specific derogations for certain situations. The other options are not the first steps to take, although they may be relevant at later stages of the data transfer process. References =

Guide to the cross-border transfer of personal data in the GDPR New guidance issued by the EDPB on international transfers of personal data Requirements for transferring personal information across borders

NO.4 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: A

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

NO.5 Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

A. hand over the controls to the relevant business owners.

B. ensure the controls are regularly tested for ongoing effectiveness.

C. perform testing to compare control performance against industry levels.

D. prepare to adapt the controls for future system upgrades.

Answer: B

NO.6 Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?

A. Review compliance requirements.

B. Communicate the exposure.

C. Declare an incident.

D. Change the encryption keys.

Answer: C

Explanation:

Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.

References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

NO.7 Which of the following BEST facilitates effective strategic alignment of security initiatives?

A. The business strategy is periodically updated

B. Procedures and standards are approved by department heads.

C. Periodic security audits are conducted by a third-party.

D. Organizational units contribute to and agree on priorities

Answer: D

Explanation:

Organizational units contribute to and agree on priorities is the best way to facilitate effective strategic alignment of security initiatives because it ensures that the security initiatives are aligned with the business goals and objectives, supported by relevant stakeholders, and prioritized based on risk and value. The business strategy is periodically updated is not sufficient to facilitate effective strategic alignment of security initiatives because it does not involve collaboration or communication between different organizational units.

Procedures and standards are approved by department heads is not sufficient to facilitate effective strategic alignment of security initiatives because it does not reflect the strategic direction or vision of the organization.

Periodic security audits are conducted by a third-party is not sufficient to facilitate effective strategic alignment of security initiatives because it does not address the planning or implementation of security initiatives. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align- security-initiatives-with-business-goals-and-objectives

https://www.isaca.org/resources/isaca-journal/issues

/2015/volume-1/how-to-measure-the-effectiveness-of-information-security-governance

NO.8 Which of the following is the MOST important reason to consider organizational culture when developing an information security program?

A. Everyone in the organization is responsible for information security.
B. It helps expedite approval for the information security budget.
C. It helps the organization meet compliance requirements.
D. Security incidents have an adverse impact on the entire organization.
Answer: A

NO.9 What should be the FIRST step when an Internet of Things (IoT) device in an organization's network is confirmed to have been hacked?
A. Monitor the network.
B. Perform forensic analysis.
C. Disconnect the device from the network,
D. Escalate to the incident response team
Answer: C
Explanation:
= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network.
Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures123. References =
1: CISM Review Manual 15th Edition, page 2004
2: CISM Practice Quiz, question 1072
3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

NO.10 The GREATEST challenge when attempting data recovery of a specific file during forensic analysis is when:
A. the partition table on the disk has been deleted.
B. the tile has been overwritten.
C. all files in the directory have been deleted.
D. high-level disk formatting has been performed.
Answer: B
Explanation:
Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.
Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.
However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools.
References = CISM Review Manual,
16th Edition, Chapter 5, Section 5.4.1.2

NO.11 Which of the following will provide the MOST guidance when deciding the level of protection

for an information asset?

A. Impact on information security program

B. Cost of controls

C. Impact to business function

D. Cost to replace

Answer: C

Explanation:

The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.

Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset. Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization. References = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693 When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture.

Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

NO.12 Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?

A. Include security requirements in the contract.

B. Update the risk register.

C. Consult with the business owner.

D. Restrict application network access temporarily.

Answer: C

Explanation:

Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of

action, such as modifying the requirements, finding an alternative solution, or accepting the risk.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: "The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications." CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third- party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk." Best Practices to Manage Risks in the Cloud - ISACA: "The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance."

NO.13 An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk?

A. Requirement for regular information security awareness

B. Right-to-audit clause

C. Service level agreement (SLA)

D. Requirement to comply with corporate security policy

Answer: D

Explanation:
The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.
References = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NO.14 An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy, A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

A. the chief risk officer (CRO).

B. business senior management.

C. the information security manager.

D. the compliance officer.

Answer: B

Explanation:
Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel,

and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.
The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The information security manager is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

NO.15 When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager?

A. Managing the impact

B. Identifying unacceptable risk levels

C. Assessing vulnerabilities

D. Evaluating potential threats

Answer: A

Explanation:
When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. References:
https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/
https://www.osha.gov/safety-management/hazard-prevention
https://www.cdc.gov/niosh/topics/hierarchy/default.html

NO.16 Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?

A. The capabilities and expertise of the information security team

B. The organization's mission statement and roadmap

C. A prior successful information security strategy

D. The organization's information technology (IT) strategy

Answer: B

Explanation:

= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security strategy with them. The information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes.

The capabilities and expertise of the information security team (A) are important factors for the information security manager to consider, but they are not the most useful source of information for developing and implementing an information security strategy. The information security team is responsible for executing and maintaining the information security program and activities, such as risk management, security awareness, incident response, and compliance. The information security manager should assess the capabilities and expertise of the information security team to identify the strengths, weaknesses, opportunities, and threats, and to plan the resource allocation, training, and development of the team. However, the capabilities and expertise of the information security team do not directly inform the information security strategy, which should be driven by the organization's business objectives, risk appetite, and security needs.

A prior successful information security strategy is a possible source of information for the information security manager to refer to, but it is not the most useful one. A prior successful information security strategy is a strategy that has been implemented and evaluated by another organization or a previous information security manager, and has achieved the desired security outcomes and benefits. The information security manager can learn from the best practices, lessons learned, and challenges of a prior successful information security strategy, and apply them to the current organization or situation. However, a prior successful information security strategy may not be relevant, applicable, or suitable for the organization, as it may not reflect the current or future business objectives, risk appetite, and security needs of the organization, or the changing threat landscape and business environment.

The organization's information technology (IT) strategy (D) is also a possible source of information for the information security manager to consult, but it is not the most useful one. The IT strategy is a strategy that defines the IT vision, goals, and initiatives of the organization, and how IT supports and enables the business processes and activities. The information security manager should review the IT strategy to understand the IT infrastructure, systems, and services of the organization, and how they relate to the information security program and activities. However, the IT strategy is not the primary driver of the information security strategy, which should be aligned with the organization's business objectives, risk appetite, and security needs, and not only with the IT objectives, capabilities, and

requirements.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy Development, page 23-241

NO.17 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.

NO.18 A security review identifies that confidential information on the file server has been accessed by unauthorized users in the organization. Which of the following should the information security manager do FIRST?
A. Invoke the incident response plan
B. Implement role-based access control (RBAC)
C. Remove access to the information
D. Delete the information from the file server
Answer: A
Explanation:

The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.
"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution* ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

NO.19 Which of the following is the BEST way to enhance training for incident response teams?

A. Perform post-incident reviews.

B. Establish incident key performance indicators (KPIs).

C. Conduct interviews with organizational units.

D. Participate in emergency response activities.

Answer: A

Explanation:
Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.
References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

NO.20 Which of the following is MOST important for an organization to have in place to determine the effectiveness of information security governance?

A. Program metrics

B. Key risk indicators (KRIs)

C. Risk register

D. Security strategy

Answer: A

Explanation:
Program metrics measure the effectiveness of governance processes and provide a basis for continuous improvement and informed decision-making.
"Metrics are essential for evaluating governance performance, demonstrating effectiveness, and identifying areas for improvement."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Monitoring and Metrics* ISACA's practice questions confirm that program metrics are key to evaluating governance effectiveness.

NO.21 An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?

A. Include security requirements in the contract

B. Assess security controls.

C. Perform a risk assessment

D. Review data architecture.

Answer: C

Explanation:

Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NO.22 When evaluating cloud storage solutions, the FIRST consideration should be:

A. The service level agreement (SLA) for encryption keys

B. Alignment with the organization's data classification policy

C. How the organization's sensitive data will be transferred

D. The volume of data to be stored in the cloud

Answer: B

Explanation:

The first consideration when evaluating cloud storage solutions is alignment with the organization's data classification policy (B). CISM emphasizes that security requirements must be driven by data sensitivity and business value. Before assessing encryption methods, SLAs, or data transfer mechanisms, the organization must determine what type of data will be stored and what protection level is required. Data classification informs confidentiality, integrity, availability, privacy, and regulatory requirements. Evaluating SLAs (A) or transfer methods (C) without understanding data sensitivity risks misalignment with governance and compliance obligations. Data volume (D) is an operational consideration, not a security driver.

References: ISACA CISM Review Manual (Risk management-data classification, cloud risk evaluation); CISM Exam Content Outline (Domain 1).

NO.23 Which of the following BEST helps to ensure a third-party backup site continues to meet the organization's information security standards?

A. Service level agreement (SLA)

B. Memorandum of understanding (MoU)

C. Business continuity plan (BCP)

D. Disaster recovery plan (DRP)

Answer: A
Explanation:
A Service Level Agreement (SLA) is a legally binding document that defines the performance and compliance expectations for third-party services, including information security requirements. It is the best mechanism to ensure that the third-party backup site meets ongoing security standards.
"SLAs should include security, availability, and performance expectations to align third-party services with organizational policies."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Third-Party Relationships*

NO.24 Which of the following is MOST important to the successful implementation of an information security program?

A. Adequate security resources are allocated to the program.

B. Key performance indicators (KPIs) are defined.

C. A balanced scorecard is approved by the steering committee.

D. The program is developed using global security standards.

Answer: A
Explanation:
The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives, comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.
References = CISM Review Manual, 16th Edition, page 69

NO.25 When designing security controls, it is MOST important to:

A. Apply a risk-based approach

B. Apply technical controls for sensitive data

C. Consider business impact analysis (BIA) results

D. Focus on preventive controls

Answer: A
Explanation:
A risk-based approach (A) is fundamental to control design in CISM. Controls must be proportionate to risk, aligned with business objectives, and consistent with risk appetite. Focusing solely on technical controls (B), BIA results (C), or preventive controls (D) limits effectiveness. A risk-based approach ensures balanced use of preventive, detective, and corrective controls.
References: ISACA CISM Review Manual (Risk management-control selection); CISM Exam Content Outline (Domain 1).

NO.26 Which of the following is the MOST important consideration when determining which type of failover site to employ?

A. Reciprocal agreements

B. Disaster recovery test results

C. Recovery time objectives (RTOs)

D. Data retention requirements

Answer: C

Explanation:

The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources.

Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

NO.27 A backdoor has been identified that enabled a cyberattack on an organization's systems. Integrating which of the following into the software development life cycle would BEST enable the organization to mitigate similar attacks in the future?

A. Enhanced user acceptance testing (UAT)

B. Separation of duties

C. Customized developer training

D. Vulnerability testing

Answer: D

Explanation:

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

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

NO.28 Which of the following is the BEST way to assess the risk associated with using a Software as a

Service (SaaS) vendor?

A. Verify that information security requirements are included in the contract.

B. Request customer references from the vendor.

C. Require vendors to complete information security questionnaires.

D. Review the results of the vendor's independent control reports.

Answer: D

Explanation:

Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.

Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting those requirements. The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.

Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment.

Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. References = CISM Review Manual 15th Edition, page 144 SaaS Security Risk and Challenges - ISACA1 SaaS Security Checklist & Assessment Questionnaire | LeanIX2 Risk Assessment Guide for Microsoft Cloud3

NO.29 Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?

A. Review the previous risk assessment and countermeasures.

B. Perform a new risk assessment,

C. Evaluate countermeasures to mitigate new risks.

D. Transfer the new risk to a third party.

Answer: B

Explanation:

According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A risk assessment helps to determine the current level of risk exposure and the

adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.
The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options. References = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

NO.30 Unintentional behavior by an employee caused a major data loss incident. Which of the following is the BEST way for the information security manager to prevent recurrence within the organization?
A. Implement compensating controls.
B. Communicate consequences for future instances.
C. Enhance the data loss prevention (DLP) solution.
D. Improve the security awareness training program.
Answer: D

NO.31 An online bank identifies a successful network attack in progress. The bank should FIRST:
A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (PII) is compromised.
D. shut down the entire network.
Answer: 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 (PII) is compromised, and shutting down the entire network are not the first actions that the online bank should take, as they may not be feasible or appropriate at the time of the attack, and may cause more disruption, confusion, or damage to the business operations and reputation. References = CISM Review Manual 2023, page 1641; CISM Review Questions, Answers & Explanations Manual 2023, page 362; ISACA CISM - iSecPrep, page 213

NO.32 Which of the following is the PRIMARY objective of information asset classification?
A. Vulnerability reduction
B. Compliance management
C. Risk management
D. Threat minimization
Answer: C

Explanation:
The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security. Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

NO.33 Which of the following is the BEST indication of a mature information security program?

A. Security incidents are managed properly.

B. Security spending is below budget.

C. Security resources are optimized.

D. Security audit findings are reduced.

Answer: C

Explanation:
A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

NO.34 Which of the following is the BEST indication of an effective disaster recovery planning process?

A. Hot sites are required for any declared disaster.

B. Chain of custody is maintained throughout the disaster recovery process.

C. Post-incident reviews are conducted after each event.

D. Recovery time objectives (RTOs) are shorter than recovery point objectives (RPOs).

Answer: C

NO.35 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_Booklet.pdf
https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d