Number: CISM
Passing Score: 800.0
Time Limit: 120.0
File Version: 21.0

**Exam Code: CISM**
**Exam Name: Certified Information Security Manager**

**Exam A**

**QUESTION 1**
Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

A. Intrusion detection
B. Log monitoring
C. Patch management
D. Antivirus software

**Correct Answer: C**
**Section:**

**QUESTION 2**
Which of the following is the FIRST step to establishing an effective information security program?

A. Conduct a compliance review.
B. Assign accountability.
C. Perform a business impact analysis (BIA).
D. Create a business case.

**Correct Answer: D**
**Section:**

**QUESTION 3**
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.

**Correct Answer: B**
**Section:**

**QUESTION 4**
Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

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

**Correct Answer: C**
**Section:**

**QUESTION 5**
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

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

**Correct Answer: C**
**Section:**

**QUESTION 6**
Which of the following is the BEST indicator of an organization's information security status?

A. Intrusion detection log analysis
B. Controls audit
C. Threat analysis
D. Penetration test

**Correct Answer: B**
**Section:**

**QUESTION 7**
An organization recently outsourced the development of a mission-critical business application. Which of the following would be the BEST way to test for the existence of backdoors?

A. Scan the entire application using a vulnerability scanning tool.
B. Run the application from a high-privileged account on a test system.
C. Perform security code reviews on the entire application.
D. Monitor Internet traffic for sensitive information leakage.

**Correct Answer: C**
**Section:**

**QUESTION 8**
The PRIMARY benefit of introducing a single point of administration in network monitoring is that it:

A. reduces unauthorized access to systems.
B. promotes efficiency in control of the environment.
C. prevents inconsistencies in information in the distributed environment.
D. allows administrative staff to make management decisions.

**Correct Answer: D**
**Section:**

**QUESTION 9**
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.

**Correct Answer: C**
**Section:**

**QUESTION 10**
Which of the following is the BEST indication of an effective information security awareness training program?

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

**Correct Answer: D**
**Section:**

**QUESTION 11**
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,

**Correct Answer: A**
**Section:**

**QUESTION 12**
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.

**Correct Answer: A**
**Section:**

**QUESTION 13**
An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

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

**Correct Answer: A**
**Section:**

**QUESTION 14**
Which of the following will result in the MOST accurate controls assessment?

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

**Correct Answer: B**
**Section:**

**QUESTION 15**
An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?

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

**Correct Answer: C**
**Section:**

**QUESTION 16**
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,

**Correct Answer: D**
**Section:**

**QUESTION 17**
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?

A. Conduct an impact assessment.

B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.

**Correct Answer: B**
**Section:**

**QUESTION 18**
In which cloud model does the cloud service buyer assume the MOST security responsibility?

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

**Correct Answer: B**
**Section:**

**QUESTION 19**
In a business proposal, a potential vendor promotes being certified for international security standards as a measure of its security capability. Before relying on this certification, it is MOST important that the information security manager confirms that the:

A. current international standard was used to assess security processes.
B. certification will remain current through the life of the contract.
C. certification scope is relevant to the service being offered.
D. certification can be extended to cover the client's business.

**Correct Answer: C**
**Section:**

**QUESTION 20**
Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

A. Management's business goals and objectives
B. Strategies of other non-regulated companies
C. Risk assessment results
D. Industry best practices and control recommendations

**Correct Answer: A**
**Section:**

**QUESTION 21**
When investigating an information security incident, details of the incident should be shared:

A. widely to demonstrate positive intent.
B. only with management.
C. only as needed,

D. only with internal audit.

**Correct Answer: C**
**Section:**

**QUESTION 22**
Which of the following should be the PRIMARY consideration when developing an incident response plan?

A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents

**Correct Answer: B**
**Section:**

**QUESTION 23**
An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?

A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.

**Correct Answer: B**
**Section:**

**QUESTION 24**
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?

A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule

**Correct Answer: C**
**Section:**

**QUESTION 25**
What is the BEST way to reduce the impact of a successful ransomware attack?

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

**Correct Answer: A**
**Section:**

**QUESTION 26**
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.

**Correct Answer: B**
**Section:**

**QUESTION 27**
Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA
B. To increase awareness of information security among key stakeholders
C. To ensure the stakeholders providing input own the related risk
D. To obtain input from as many relevant stakeholders as possible

**Correct Answer: C**
**Section:**

**QUESTION 28**
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

**Correct Answer: A**
**Section:**

**QUESTION 29**
Which of the following is the BEST course of action for an information security manager to align security and business goals?

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

**Correct Answer: D**
**Section:**

**QUESTION 30**
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

**Correct Answer: D**
**Section:**

**QUESTION 31**
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

**Correct Answer: B**
**Section:**

**QUESTION 32**
Which of the following is MOST important when conducting a forensic investigation?

A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody

**Correct Answer: D**
**Section:**

**QUESTION 33**
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.

**Correct Answer: D**
**Section:**

**QUESTION 34**
Which of the following BEST indicates that information security governance and corporate governance are integrated?

A. The information security team is aware of business goals.
B. The board is regularly informed of information security key performance indicators (KPIs),
C. The information security steering committee is composed of business leaders.
D. A cost-benefit analysis is conducted on all information security initiatives.

**Correct Answer: C**
**Section:**

**QUESTION 35**
Management decisions concerning information security investments will be MOST effective when they are based on:

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

**Correct Answer: C**
**Section:**

**QUESTION 36**
Which of the following service offerings in a typical Infrastructure as a Service (laaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?

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

**Correct Answer: D**
**Section:**

**QUESTION 37**
When developing an asset classification program, which of the following steps should be completed FIRST?

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

**Correct Answer: B**
**Section:**

**QUESTION 38**
A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.

D. Initiate the organization's incident response process.

**Correct Answer: C**
**Section:**

**QUESTION 39**
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

**Correct Answer: B**
**Section:**

**QUESTION 40**
An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?

A. Create a business case for a new incident response plan.
B. Revise the existing incident response plan.
C. Conduct a gap analysis.
D. Assess the impact to the budget,

**Correct Answer: C**
**Section:**

**QUESTION 41**
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

**Correct Answer: A**
**Section:**

**QUESTION 42**
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

**Correct Answer: C**

**Section:**

**QUESTION 43**
Which of the following is the PRIMARY reason for granting a security exception?

A. The risk is justified by the cost to the business.
B. The risk is justified by the benefit to security.
C. The risk is justified by the cost to security.
D. The risk is justified by the benefit to the business.

**Correct Answer: D**
**Section:**

**QUESTION 44**
An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?

A. Determine which country's information security regulations will be used.
B. Merge the two existing information security programs.
C. Apply the existing information security program to the acquired company.
D. Evaluate the information security laws that apply to the acquired company.

**Correct Answer: D**
**Section:**

**QUESTION 45**
An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

A. Red team exercise
B. Black box penetration test
C. Disaster recovery exercise
D. Tabletop exercise

**Correct Answer: D**
**Section:**

**QUESTION 46**
Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

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

**Correct Answer: C**
**Section:**

**QUESTION 47**

Which of the following is the BEST way to achieve compliance with new global regulations related to the protection of personal information?

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

**Correct Answer: D**
**Section:**

**QUESTION 48**
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

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

**Correct Answer: B**
**Section:**

**QUESTION 49**
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.

**Correct Answer: A**
**Section:**

**QUESTION 50**
Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.

**Correct Answer: C**
**Section:**

**QUESTION 51**
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

**Correct Answer: A**
**Section:**

**QUESTION 52**
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?

A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes

**Correct Answer: D**
**Section:**

**QUESTION 53**
Which of the following is MOST important for building 4 robust information security culture within an organization?

A. Mature information security awareness training across the organization
B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies

**Correct Answer: D**
**Section:**

**QUESTION 54**
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.

**Correct Answer: A**
**Section:**

**QUESTION 55**
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

**Correct Answer: C**
**Section:**

**QUESTION 56**
A recovery point objective (RPO) is required in which of the following?

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

**Correct Answer: A**
**Section:**

**QUESTION 57**
What should be the FIRST step when an Internet of Things (loT) device in an organization's network is confirmed to have been hacked?

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

**Correct Answer: C**
**Section:**

**QUESTION 58**
An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

A. a control self-assessment (CSA) process.
B. automated reporting to stakeholders.
C. a monitoring process for the security policy.
D. metrics for each milestone.

**Correct Answer: D**
**Section:**

**QUESTION 59**
Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.

**Correct Answer: B**
**Section:**

**QUESTION 60**
Which of the following BEST enables staff acceptance of information security policies?

A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program
D. Adequate security funding

**Correct Answer: A**
**Section:**

**QUESTION 61**
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?

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

**Correct Answer: B**
**Section:**

**QUESTION 62**
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?

A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.

**Correct Answer: A**
**Section:**

**QUESTION 63**
Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?

A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk

**Correct Answer: C**
**Section:**

**QUESTION 64**
An organization's disaster recovery plan (DRP) is documented and kept at a disaster recovery site. Which of the following is the BEST way to ensure the plan can be carried out in an emergency?

A. Store disaster recovery documentation in a public cloud.
B. Maintain an outsourced contact center in another country.
C. Require disaster recovery documentation be stored with all key decision makers.
D. Provide annual disaster recovery training to appropriate staff.

**Correct Answer: C**
**Section:**

**QUESTION 65**
Information security controls should be designed PRIMARILY based on:

A. a business impact analysis (BIA).
B. regulatory requirements.
C. business risk scenarios,
D. a vulnerability assessment.

**Correct Answer: C**
**Section:**

**QUESTION 66**
Which of the following is the BEST indication that an organization has a mature information security culture?

A. Information security training is mandatory for all staff.
B. The organization's information security policy is documented and communicated.
C. The chief information security officer (CISO) regularly interacts with the board.
D. Staff consistently consider risk in making decisions.

**Correct Answer: D**
**Section:**
**Explanation:**
The BEST indication that an organization has a mature information security culture is when its staff consistently consider risk in making decisions. When an organization's staff understands the risks associated with their actions and are empowered to make risk-informed decisions, it indicates that the organization has a mature information security culture.
According to the Certified Information Security Manager (CISM) Study Manual, 'A mature information security culture exists when the people within the organization understand and appreciate the risks associated with information and technology and when they take steps to manage those risks on a daily basis.'
While information security training, documented information security policies, and regular interaction between the chief information security officer (CISO) and the board are all important components of a mature information security culture, they are not sufficient on their own. It is only when staff consistently consider risk in making decisions that an organization's information security culture can be considered mature.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 151-152.

**QUESTION 67**
What is the PRIMARY benefit to an organization that maintains an information security governance framework?

A. Resources are prioritized to maximize return on investment (ROI)
B. Information security guidelines are communicated across the enterprise_
C. The organization remains compliant with regulatory requirements.
D. Business risks are managed to an acceptable level.

**Correct Answer: D**

**Section:**
**Explanation:**
According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.
Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.
According to the Certified Information Security Manager (CISM) Study Manual, 'Information security governance provides a framework for managing and controlling information security practices and technologies at an enterprise level. Its primary objective is to manage and reduce risk through a process of identification, assessment, and management of those risks.'
While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

**QUESTION 68**
Which of the following would be MOST effective in gaining senior management approval of security investments in network infrastructure?

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

**Correct Answer: C**
**Section:**
**Explanation:**
The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives.
Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.
According to the Certified Information Security Manager (CISM) Study Manual, 'To gain senior management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization.'
While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

**QUESTION 69**
Which of the following should be the PRIMARY objective of an information security governance framework?

A. Provide a baseline for optimizing the security profile of the organization.
B. Demonstrate senior management commitment.
C. Demonstrate compliance with industry best practices to external stakeholders.
D. Ensure that users comply with the organization's information security policies.

**Correct Answer: A**
**Section:**
**Explanation:**
According to the Certified Information Security Manager (CISM) Study Manual, 'The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks.'
While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 60.

**QUESTION 70**
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.

**Correct Answer: A**
**Section:**
**Explanation:**
The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans.
Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

**QUESTION 71**
Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?

A. Providing training from third-party forensics firms
B. Obtaining industry certifications for the response team
C. Conducting tabletop exercises appropriate for the organization
D. Documenting multiple scenarios for the organization and response steps

**Correct Answer: C**
**Section:**
**Explanation:**
The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.
According to the Certified Information Security Manager (CISM) Study Manual, 'Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan.'
While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

**QUESTION 72**
An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

A. The information security manager
B. The data owner
C. The application owner
D. The security engineer

**Correct Answer: B**
**Section:**

**QUESTION 73**
Network isolation techniques are immediately implemented after a security breach to:

A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.

**Correct Answer: B**
**Section:**

**QUESTION 74**
Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

A. Enable multi-factor authentication on user and admin accounts.
B. Review access permissions annually or whenever job responsibilities change
C. Lock out accounts after a set number of unsuccessful login attempts.
D. Delegate the management of access permissions to an independent third party.

**Correct Answer: B**
**Section:**

**QUESTION 75**
The PRIMARY advantage of involving end users in continuity planning is that they:

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

**Correct Answer: A**
**Section:**

**QUESTION 76**
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

**Correct Answer: B**
**Section:**

**QUESTION 77**
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

**Correct Answer: B**
**Section:**

**QUESTION 78**
Which of the following is MOST effective in monitoring an organization's existing risk?

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

**Correct Answer: B**
**Section:**

**QUESTION 79**
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

**Correct Answer: B**
**Section:**

**QUESTION 80**
Of the following, who is in the BEST position to evaluate business impacts?

A. Senior management
B. Information security manager
C. IT manager
D. Process manager

**Correct Answer: D**
**Section:**

**QUESTION 81**
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.

**Correct Answer: B**
**Section:**

**QUESTION 82**
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,

**Correct Answer: C**
**Section:**

**QUESTION 83**
Which of the following MUST happen immediately following the identification of a malware incident?

A. Preparation
B. Recovery
C. Containment
D. Eradication

**Correct Answer: B**
**Section:**

**QUESTION 84**
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?

A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products
D. Unreliable delivery of hardware and software resources by a supplier

**Correct Answer: C**
**Section:**

**QUESTION 85**
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).

**Correct Answer: C**

**Section:**

**QUESTION 86**
A PRIMARY purpose of creating security policies is to:

A. define allowable security boundaries.
B. communicate management's security expectations.
C. establish the way security tasks should be executed.
D. implement management's security governance strategy.

**Correct Answer: B**
**Section:**

**QUESTION 87**
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

**Correct Answer: C**
**Section:**

**QUESTION 88**
Which of the following is the PRIMARY reason to monitor key risk indicators (KRIs) related to information security?

A. To alert on unacceptable risk
B. To identify residual risk
C. To reassess risk appetite
D. To benchmark control performance

**Correct Answer: D**
**Section:**

**QUESTION 89**
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.

**Correct Answer: B**
**Section:**

**QUESTION 90**

Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?

A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.
D. Identify recovery time objectives (RTOs).

**Correct Answer: A**
**Section:**

**QUESTION 91**
In violation of a policy prohibiting the use of cameras at the office, employees have been issued smartphones and tablet computers with enabled web cameras. Which of the following should be the information security manager's FIRST course of action?

A. Revise the policy.
B. Perform a root cause analysis.
C. Conduct a risk assessment,
D. Communicate the acceptable use policy.

**Correct Answer: C**
**Section:**

**QUESTION 92**
Which of the following is an information security manager's MOST important course of action when responding to a major security incident that could disrupt the business?

A. Follow the escalation process.
B. Identify the indicators of compromise.
C. Notify law enforcement.
D. Contact forensic investigators.

**Correct Answer: B**
**Section:**

**QUESTION 93**
Which of the following would be MOST helpful to identify worst-case disruption scenarios?

A. Business impact analysis (BIA)
B. Business process analysis
C. SWOT analysis
D. Cast-benefit analysis

**Correct Answer: A**
**Section:**
**Explanation:**
Topic 2, Exam Pool B

**QUESTION 94**

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. results of exit interviews.
B. previous training sessions.
C. examples of help desk requests.
D. responses to security questionnaires.

**Correct Answer: C**
**Section:**

**QUESTION 95**
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)

**Correct Answer: B**
**Section:**

**QUESTION 96**
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

**Correct Answer: D**
**Section:**

**QUESTION 97**
A Seat a-hosting organization's data center houses servers, appli
BEST approach for developing a physical access control policy for the organization?

A. Review customers' security policies.
B. Conduct a risk assessment to determine security risks and mitigating controls.
C. Develop access control requirements for each system and application.
D. Design single sign-on (SSO) or federated access.

**Correct Answer: B**
**Section:**

**QUESTION 98**
Which of the following would BEST help to ensure appropriate security controls are built into software?

A. Integrating security throughout the development process
B. Performing security testing prior to deployment
C. Providing standards for implementation during development activities
D. Providing security training to the software development team

**Correct Answer: C**
**Section:**

**QUESTION 99**
Which of the following will ensure confidentiality of content when accessing an email system over the Internet?

A. Multi-factor authentication
B. Digital encryption
C. Data masking
D. Digital signatures

**Correct Answer: B**
**Section:**

**QUESTION 100**
What should be an information security manager's MOST important consideration when developing a multi-year plan?

A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year

**Correct Answer: B**
**Section:**

**QUESTION 101**
Reevaluation of risk is MOST critical when there is:

A. resistance to the implementation of mitigating controls.
B. a management request for updated security reports.
C. a change in security policy.
D. a change in the threat landscape.

**Correct Answer: D**
**Section:**

**QUESTION 102**
Which of the following is MOST effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application?

A. A patch management process
B. Version control
C. Change management controls

D. Logical access controls

**Correct Answer: A**
**Section:**

**QUESTION 103**
An organization is creating a risk mitigation plan that considers redundant power supplies to reduce the business risk associated with critical system outages. Which type of control is being considered?

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

**Correct Answer: A**
**Section:**

**QUESTION 104**
What is the PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes?

A. Security incident reporting procedures are followed.
B. Security staff turnover is reduced.
C. Information assets are classified appropriately.
D. Access is granted based on task requirements.

**Correct Answer: D**
**Section:**

**QUESTION 105**
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?

A. Document risk acceptances.
B. Revise the organization's security policy.
C. Assess the consequences of noncompliance.
D. Conduct an information security audit.

**Correct Answer: C**
**Section:**

**QUESTION 106**
To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:

A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.
D. right to audit is included in the service level agreement (SLA).

**Correct Answer: D**

**Section:**

**QUESTION 107**
Which of the following is MOST important to include in monthly information security reports to the board?

A. Trend analysis of security metrics
B. Risk assessment results
C. Root cause analysis of security incidents
D. Threat intelligence

**Correct Answer: A**
**Section:**

**QUESTION 108**
Which of the following should be the PRIMARY basis for determining the value of assets?

A. Cost of replacing the assets
B. Business cost when assets are not available
C. Original cost of the assets minus depreciation
D. Total cost of ownership (TCO)

**Correct Answer: B**
**Section:**

**QUESTION 109**
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

**Correct Answer: B**
**Section:**

**QUESTION 110**
Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?

A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan

**Correct Answer: C**
**Section:**

**QUESTION 111**

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. Process owners
B. End users
C. Security architects.
D. Corporate auditors

**Correct Answer: A**
**Section:**

**QUESTION 112**
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

**Correct Answer: A**
**Section:**

**QUESTION 113**
Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?

A. Decrease in the number of security incidents
B. Increase in the frequency of security incident escalations
C. Reduction in the impact of security incidents
D. Increase in the number of reported security incidents

**Correct Answer: A**
**Section:**

**QUESTION 114**
Which of the following should be the MOST important consideration of business continuity management?

A. Ensuring human safety
B. Identifying critical business processes
C. Ensuring the reliability of backup data
D. Securing critical information assets

**Correct Answer: A**
**Section:**

**QUESTION 115**
A user reports a stolen personal mobile device that stores sensitive corporate dat

A. Which of the following will BEST minimize the risk of data exposure?

B. Prevent the user from using personal mobile devices.
C. Report the incident to the police.
D. Wipe the device remotely.
E. Remove user's access to corporate data.

**Correct Answer: C**
**Section:**

**QUESTION 116**
Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.
B. Internal compliance requirements are being met.
C. Risk management objectives are being met.
D. Business needs are being met.

**Correct Answer: D**
**Section:**

**QUESTION 117**
Which of the following is the BEST approach to incident response for an organization migrating to a cloud-based solution?

A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.

**Correct Answer: D**
**Section:**

**QUESTION 118**
Which of the following is the BEST indication of effective information security governance?

A. Information security is considered the responsibility of the entire information security team.
B. Information security controls are assigned to risk owners.
C. Information security is integrated into corporate governance.
D. Information security governance is based on an external security framework.

**Correct Answer: C**
**Section:**

**QUESTION 119**
Which of the following is the BEST way to obtain support for a new organization-wide information security program?

A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.

D. Establish an information security strategy committee.

**Correct Answer: B**
**Section:**
**Explanation:**
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

**QUESTION 120**
Which of the following backup methods requires the MOST time to restore data for an application?

A. Full backup
B. Incremental
C. Differential
D. Disk mirroring

**Correct Answer: A**
**Section:**
**Explanation:**
The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

**QUESTION 121**
The PRIMARY purpose for continuous monitoring of security controls is to ensure:

A. control gaps are minimized.
B. system availability.
C. effectiveness of controls.
D. alignment with compliance requirements.

**Correct Answer: C**
**Section:**
**Explanation:**
The primary purpose for continuous monitoring of security controls is to ensure the effectiveness of controls. This involves regularly assessing the controls to ensure that they are meeting their intended objectives, and that any potential weaknesses are identified and addressed. Continuous monitoring also helps to ensure that control gaps are minimized, and that systems are available and aligned with compliance requirements.

**QUESTION 122**
Which of the following is the GREATEST value provided by a security information and event management (SIEM) system?

A. Maintaining a repository base of security policies
B. Measuring impact of exploits on business processes
C. Facilitating the monitoring of risk occurrences
D. Redirecting event logs to an alternate location for business continuity plan

**Correct Answer: C**
**Section:**

**Explanation:**
The greatest value provided by a Security Information and Event Management (SIEM) system is facilitating the monitoring of risk occurrences. SIEM systems collect, analyze and alert on security-related data from various sources such as firewall logs, intrusion detection/prevention systems, and system logs. This allows organizations to identify security threats in real-time and respond quickly, helping to mitigate potential harm to their systems and data.

**QUESTION 123**
An organization's quality process can BEST support security management by providing:

A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.

**Correct Answer: B**
**Section:**
**Explanation:**
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

**QUESTION 124**
A newly appointed information security manager of a retailer with multiple stores discovers an HVAC (heating, ventilation, and air conditioning) vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. Which of the following should be the information security manager's FIRST course of action?

A. Conduct a penetration test of the vendor.
B. Review the vendor's technical security controls
C. Review the vendor contract
D. Disconnect the real-time access

**Correct Answer: C**
**Section:**
**Explanation:**
Reviewing the vendor contract should be the information security manager's first course of action when discovering an HVAC vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. The vendor contract should specify the terms and conditions of the vendor's access to the retailer's network, such as the scope, purpose, duration, frequency, and method of access. The vendor contract should also define the roles and responsibilities of both parties regarding security, privacy, compliance, liability, and incident response. Reviewing the vendor contract will help the information security manager to understand the contractual obligations and expectations of both parties, and to identify any gaps or issues that need to be addressed or resolved1. The other options are not the first course of action for the information security manager when discovering an HVAC vendor has remote access to the stores. Conducting a penetration test of the vendor may be a useful way to assess the vendor's security posture and potential vulnerabilities, but it should be done with the vendor's consent and cooperation, and after reviewing the vendor contract2. Reviewing the vendor's technical security controls may be a necessary step to verify the vendor's compliance with security standards and best practices, but it should be done after reviewing the vendor contract and in accordance with the agreed-upon audit procedures3. Disconnecting the real-time access may be a drastic measure that could disrupt the vendor's service delivery and violate the vendor contract, unless there is a clear and imminent threat or breach that warrants such action.
Reference: 1: Vendor Access: Addressing the Security Challenge with Urgency - BeyondTrust 2: Penetration Testing - NIST 3: Reduce Risk from Third Party Access | BeyondTrust : Third-Party Vendor Security Risk Management & Prevention

**QUESTION 125**
A balanced scorecard MOST effectively enables information security:

A. project management
B. governance.
C. performance.

D. risk management.

**Correct Answer: B**
**Section:**
**Explanation:**
A balanced scorecard most effectively enables information security govern-ance. Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress of an organization toward its strategic goals. It typically includes four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:
* Align information security objectives with business objectives and communicate them to senior management and other stakeholders
* Monitor and report on the effectiveness and efficiency of information security processes and controls
* Identify and prioritize improvement opportunities and corrective actions
* Demonstrate the value and benefits of information security investments
* Foster a culture of security awareness and continuous learning
Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality. A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Per-formance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment.
Reference: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per-formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders: Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

**QUESTION 126**
When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to:

A. the incident response process to stakeholders
B. adequately staff and train incident response teams.
C. develop effective escalation and response procedures.
D. make tabletop testing more effective.

**Correct Answer: C**
**Section:**
**Explanation:**
The primary benefit of establishing a clear definition of a security incident is that it helps to develop effective escalation and response procedures. A security incident is an event or an attempt that disrupts or threatens the normal operations, security, or privacy of an organization's information or systems1. A clear definition of a security in-cident helps to:
* Distinguish between normal and abnormal events, and between security-relevant and non-security-relevant events
* Determine the severity and impact of an incident, and the appropriate level of response
* Assign roles and responsibilities for incident detection, reporting, analysis, containment, eradication, recovery, and post-incident activities
* Establish criteria and thresholds for escalating incidents to higher authorities or external parties
* Define the communication channels and protocols for incident notification and coordina-tion
* Document the incident response process and procedures in a formal plan
According to NIST, a clear definition of a security incident is one of the key compo-nents of an effective incident response capability2. The other options are not the prima-ry benefits of establishing a clear definition of a security incident. Communicating the incident response process to stakeholders is important, but it is not the main purpose of defining a security incident. Adequately staffing and training incident response teams is essential, but it depends on other factors besides defining a security inci-dent. Making tabletop testing more effective is a possible outcome, but not a direct benefit of defining a security incident.
Reference: 2: NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide 1: NIST Glossary - Security Incident : What is a securi-ty incident? - TechTarget : 10 types of security incidents and how to handle them - TechTarget : 45 CFR 164.304 - Definitions - Electronic Code of Federal Regulations

**QUESTION 127**
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.

**Correct Answer: C**
**Section:**
**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.
Reference: 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

**QUESTION 128**
An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

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

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

**QUESTION 129**
Which of the following is an example of risk mitigation?

A. Purchasing insurance
B. Discontinuing the activity associated with the risk
C. Improving security controls
D. Performing a cost-benefit analysis

**Correct Answer: C**
**Section:**
**Explanation:**
Risk mitigation refers to the processes and strategies that organizations use to reduce the likelihood or impact of potential risks. Improving security controls is a classic example of risk mitigation. By implementing or enhancing security controls, organizations can reduce the risk of security incidents or breaches, such as data theft or unauthorized access. For example, implementing strong passwords, regularly updating software and systems, and training employees on security best practices are all ways to improve security controls and mitigate risk. Other examples of risk mitigation include implementing disaster recovery and business continuity plans, conducting regular security assessments and audits, and purchasing insurance.

**QUESTION 130**
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

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

**Correct Answer: D**
**Section:**
**Explanation:**
An incident response plan is a critical component of an organization's overall security strategy, as it provides a framework for responding to security incidents in a timely and effective manner. To ensure that incidents are responded to by the appropriate individuals, it is essential to have a detailed incident notification process that clearly outlines who is responsible for responding to different types of incidents, how incidents should be reported and escalated, and who should be notified in the event of an incident. This helps to ensure that incidents are addressed promptly and effectively, and that the right resources are brought to bear to resolve the issue. Other important elements to include in an incident response plan include a clear definition of roles and responsibilities, a list of external resources to assist with incidents, and incident response procedures, such as steps to contain, assess, and recover from incidents.

**QUESTION 131**
The PRIMARY objective of a post-incident review of an information security incident is to:

A. update the risk profile
B. minimize impact
C. prevent recurrence.
D. determine the impact

**Correct Answer: C**
**Section:**
**Explanation:**
The primary objective of a post-incident review of an information security incident is to identify the root cause of the incident and determine what can be done to prevent a similar incident from happening in the future. This process helps organizations to learn from past incidents and make improvements to their security posture to reduce the risk of future incidents. By conducting a thorough post-incident review, organizations can identify areas for improvement in their security controls, policies, and procedures, and implement changes to prevent similar incidents from happening in the future. Other important objectives of a post-incident review may include updating the risk profile, minimizing impact, and determining the impact of the incident, but the main focus should be on identifying ways to prevent recurrence.

**QUESTION 132**
While classifying information assets an information security manager notices that several production databases do not have owners assigned to them What is the BEST way to address this situation?

A. Assign responsibility to the database administrator (DBA).
B. Review the databases for sensitive content.
C. Prepare a report of the databases for senior management.
D. Assign the highest classification level to those databases.

**Correct Answer: A**
**Section:**
**Explanation:**
The best way to address this situation is to assign responsibility to the database administrator (DBA). The DBA should review the databases for sensitive content and assign the appropriate classification level to each database. This should be done in accordance with the organization's information security policies, which should outline the rules and guidelines for classifying information assets. Additionally, the information security manager should prepare a report of the databases for senior management, noting the databases that do not have owners assigned to them, as well as any other relevant information. This will help to ensure that the organization is properly managing its information assets and that any risks associated with the lack of owners are identified and addressed. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 5.3.

**QUESTION 133**
Which of the following events would MOST likely require a revision to the information security program?

A. An increase in industry threat level .
B. A significant increase in reported incidents
C. A change in IT management
D. A merger with another organization

**Correct Answer: D**
**Section:**
**Explanation:**
A merger with another organization would likely require a revision to the information security program because it can result in significant changes to the structure, size, and information systems of the merged entity. This can affect the security requirements, risk tolerance, and governance policies of the organization. To ensure that the information security program remains effective, it is important to review and revise the security policies, standards, and procedures in light of the changes brought on by the merger. The information security program should align with the new organization's risk tolerance, security requirements, and governance policies. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 3.1.

**QUESTION 134**
Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?

A. The application does not use a secure communications protocol
B. The application is configured with restrictive access controls
C. The business process has only one level of error checking
D. Server-based malware protection is not enforced

**Correct Answer: B**
**Section:**
**Explanation:**
The greatest concern for an information security manager in this situation would be the security of the data that is being processed by the third-party service provider working from a remote site. This could be a concern because the data may not be adequately protected from unauthorized access, manipulation, or theft. A secure communications protocol should be used to ensure the confidentiality and integrity of the data in transit. Additionally, the information security manager should ensure that the third-party service provider has appropriate security controls in place to protect the data, such as access controls, error checking, and malware

protection. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 5.2.

**QUESTION 135**
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?

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

**Correct Answer: C**
**Section:**
**Explanation:**
When recovering a compromised system that needs a complete rebuild, the first step should be to restore configuration management files. Configuration management files are critical for identifying the system's original state and the changes that were made to it, and restoring them can help ensure that the system is rebuilt to its original state.
According to the Certified Information Security Manager (CISM) Study Manual, 'The initial phase of the recovery process requires that configuration management files be restored. These files represent the foundation of the system and provide insight into the original state of the system, which is important for identifying changes that were made to the system as well as ensuring the recovery process can return the system to its original state.'
Patch management files, network system logs, and intrusion detection system (IDS) logs are also important in the recovery process, but they should be addressed after configuration management files have been restored.
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 256.

**QUESTION 136**
Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

A. Revisit the business objective.
B. Escalate to senior management.
C. Perform a cost-benefit analysis.
D. Recommend risk acceptance.

**Correct Answer: B**
**Section:**
**Explanation:**
Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps2. However, this answer is not certain, and you might need to consider other factors as well.

**QUESTION 137**
Which of the following is the MOST important detail to capture in an organization's risk register?

A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria
D. Risk ownership

**Correct Answer: D**
**Section:**
**Explanation:**
Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

**QUESTION 138**
Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?

A. It transfers the risk associated with recovery to a third party.
B. It lowers the annual cost to the business.
C. It eliminates the need to maintain offsite facilities.
D. It eliminates the need for the business to perform testing.

**Correct Answer: B**
**Section:**

**QUESTION 139**
Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?

A. To reduce risk mitigation costs
B. To resolve vulnerabilities in enterprise architecture (EA)
C. To manage the risk to an acceptable level
D. To eliminate threats impacting the business

**Correct Answer: C**
**Section:**
**Explanation:**
According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

**QUESTION 140**
Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?

A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats

**Correct Answer: B**
**Section:**
**Explanation:**
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

**QUESTION 141**
Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?

A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions

C. Effective protection of information assets
D. Optimized allocation of recovery resources

**Correct Answer: D**
**Section:**
**Explanation:**
The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

**QUESTION 142**
A balanced scorecard MOST effectively enables information security:

A. risk management
B. project management
C. governance
D. performance

**Correct Answer: C**
**Section:**
**Explanation:**
A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it.
A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2.It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

**QUESTION 143**
Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?

A. Embedding compliance requirements within operational processes
B. Engaging external experts to provide guidance on changes in compliance requirements
C. Performing periodic audits for compliance with legal and regulatory requirements
D. Assigning the operations manager accountability for meeting compliance requirements

**Correct Answer: A**
**Section:**
**Explanation:**
Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.
Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2.Compliance requirements may vary depending on the industry, location, and nature of the organization2.Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

**QUESTION 144**
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?

A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls

D. Ask the business owner for the new remediation plan

**Correct Answer: B**
**Section:**
**Explanation:**
The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability. This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner. The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2.A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2.A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

**QUESTION 145**
Which of the following is the MOST critical factor for information security program success?

A. comprehensive risk assessment program for information security
B. The information security manager's knowledge of the business
C. Security staff with appropriate training and adequate resources
D. Ongoing audits and addressing open items

**Correct Answer: B**
**Section:**
**Explanation:**
The explanation given in the manual is:
The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations. An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

**QUESTION 146**
Which of the following is the BEST justification for making a revision to a password policy?

A. Industry best practice
B. A risk assessment
C. Audit recommendation
D. Vendor recommendation

**Correct Answer: B**
**Section:**
**Explanation:**
A risk assessment should be conducted in order to identify the potential risks associated with a particular system or process, and to determine the best way to mitigate those risks. Making a revision to a password policy based on the results of a risk assessment is the best way to ensure that the policy is effective and secure.
According to the Certified Information Security Manager (CISM) Study manual, the BEST justification for making a revision to a password policy is a risk assessment. A risk assessment enables an organization to identify and evaluate the risks to its information assets and determine the appropriate measures to mitigate those risks, including password policies. Password policies should be based on the risks to the organization's information assets and the level of protection needed.

**QUESTION 147**
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

**Correct Answer: A**
**Section:**
**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.

**QUESTION 148**
Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?

A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure

**Correct Answer: A**
**Section:**
**Explanation:**
Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations. The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

**QUESTION 149**
Reverse lookups can be used to prevent successful:

A. denial of service (DoS) attacks
B. session hacking
C. phishing attacks
D. Internet protocol (IP) spoofing

**Correct Answer: D**

**Section:**
**Explanation:**
Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

**QUESTION 150**
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

**Correct Answer: B**
**Section:**
**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

**QUESTION 151**
Which of the following BEST demonstrates the added value of an information security program?

A. Security baselines
B. A gap analysis
C. A SWOT analysis
D. A balanced scorecard

**Correct Answer: D**
**Section:**
**Explanation:**
A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

**QUESTION 152**
Which of the following should be the FIRST step in developing an information security strategy?

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

**Correct Answer: D**
**Section:**
**Explanation:**
The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior

management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them. Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

**QUESTION 153**
Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

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

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

**QUESTION 154**
An anomaly-based intrusion detection system (IDS) operates by gathering data on:

A. normal network behavior and using it as a baseline lor measuring abnormal activity
B. abnormal network behavior and issuing instructions to the firewall to drop rogue connections
C. abnormal network behavior and using it as a baseline for measuring normal activity
D. attack pattern signatures from historical data

**Correct Answer: A**
**Section:**
**Explanation:**
An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

**QUESTION 155**
A penetration test was conducted by an accredited third party Which of the following should be the information security manager's FIRST course of action?

A. Ensure a risk assessment is performed to evaluate the findings
B. Ensure vulnerabilities found are resolved within acceptable timeframes
C. Request funding needed to resolve the top vulnerabilities
D. Report findings to senior management

**Correct Answer: D**
**Section:**

**QUESTION 156**
Which of the following is the BEST course of action when an online company discovers a network attack in progress?

A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events
D. Shut off all network access points

**Correct Answer: B**
**Section:**
**Explanation:**
The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

**QUESTION 157**
Relationships between critical systems are BEST understood by

A. evaluating key performance indicators (KPIs)
B. performing a business impact analysis (BIA)
C. developing a system classification scheme
D. evaluating the recovery time objectives (RTOs)

**Correct Answer: B**
**Section:**
**Explanation:**
The explanation given is: ''A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems.''

**QUESTION 158**
To help ensure that an information security training program is MOST effective its contents should be

A. focused on information security policy.
B. aligned to business processes
C. based on employees' roles
D. based on recent incidents

**Correct Answer: C**
**Section:**
**Explanation:**
''An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees.''

**QUESTION 159**
Which of the following should be an information security manager's FIRST course of action when a newly introduced privacy regulation affects the business?

A. Consult with IT staff and assess the risk based on their recommendations
B. Update the security policy based on the regulatory requirements
C. Propose relevant controls to ensure the business complies with the regulation

D. Identify and assess the risk in the context of business objectives

**Correct Answer: D**
**Section:**
**Explanation:**
Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

**QUESTION 160**
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

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

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

**QUESTION 161**
Which of the following is the responsibility of a risk owner?

A. Performing risk assessments to direct risk response
B. Determining the organization's risk appetite
C. Ensuring control effectiveness is monitored
D. Implementing controls to mitigate the risk

**Correct Answer: D**
**Section:**
**Explanation:**
A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk. While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

**QUESTION 162**
Which of the following is the MOST important requirement for a successful security program?

A. Mapping security processes to baseline security standards
B. Penetration testing on key systems
C. Management decision on asset value
D. Nondisclosure agreements (NDA) with employees

**Correct Answer: C**
**Section:**

**Explanation:**
''A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value.''

**QUESTION 163**
Following a risk assessment, an organization has made the decision to adopt a bring your own device (BYOD) strategy. What should the information security manager do NEXT?

A. Develop a personal device policy
B. Implement a mobile device management (MDM) solution
C. Develop training specific to BYOD awareness
D. Define control requirements

**Correct Answer: D**
**Section:**
**Explanation:**
Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.
https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating
https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

**QUESTION 164**
Which of the following is BEST used to determine the maturity of an information security program?

A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics

**Correct Answer: D**
**Section:**
**Explanation:**
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes. Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing-information-security

**QUESTION 165**
Which of the following is the BEST way to reduce the risk of security incidents from targeted email attacks?

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

**Correct Answer: C**

**Section:**
**Explanation:**
Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks. Therefore, conducting awareness training across the organization is the correct answer.
https://almanac.upenn.edu/articles/one-step-ahead-dont-get-caught-by-targeted-email-attacks
https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html

**QUESTION 166**
When implementing a security policy for an organization handling personally identifiable information (PII); the MOST important objective should be:

A. strong encryption
B. regulatory compliance.
C. data availability.
D. security awareness training

**Correct Answer: B**
**Section:**
**Explanation:**
Regulatory compliance is the most important objective when implementing a security policy for an organization handling personally identifiable information (PII) because it helps to ensure that the organization meets the legal and ethical obligations to protect the privacy and security of PII. PII is any information that can be used to identify, contact, or locate an individual, such as name, address, email, phone number, social security number, etc. PII is subject to various laws and regulations in different jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Failing to comply with these regulations can result in fines, lawsuits, reputational damage, or loss of trust. Therefore, regulatory compliance is the correct answer.
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en
https://www.digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise
https://blog.rsisecurity.com/how-to-make-a-personally-identifiable-information-policy/

**QUESTION 167**
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

A. Employee training on ransomware
B. A properly tested offline backup system
C. A continual server replication process
D. A properly configured firewall

**Correct Answer: B**
**Section:**
**Explanation:**
The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures. Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware. However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable. A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server.However, it

does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

**QUESTION 168**
An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

A. Initiate incident response.
B. Disable remote
C. Initiate a device reset.
D. Conduct a risk assessment.

**Correct Answer: A**
**Section:**
**Explanation:**
Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage. According to ISACA, incident management is one of the key processes for information security governance. Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan.
Reference: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

**QUESTION 169**
When developing a business case to justify an information security investment, which of the following would BEST enable an informed decision by senior management?

A. The information security strategy
B. Losses due to security incidents
C. The results of a risk assessment
D. Security investment trends in the industry

**Correct Answer: C**
**Section:**
**Explanation:**
The results of a risk assessment would best enable an informed decision by senior management when developing a business case to justify an information security investment. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the organization's assets and processes, as well as the potential impact and likelihood of occurrence. A risk assessment will also provide a basis for selecting and evaluating the effectiveness of controls to mitigate the risks. According to CISA, developing a business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment1. The information security strategy, losses due to security incidents, and security investment trends in the industry are possible inputs or outputs of a risk assessment, but they are not sufficient to enable an informed decision by senior management.
Reference: 1: The Business Case for Security - CISA 2: The Business Case for Security | CISA 3: #HowTo: Build a Business Case for Cybersecurity Investment 4: Making the Business Case for Information Security

**QUESTION 170**
Which risk is introduced when using only sanitized data for the testing of applications?

A. Data loss may occur during the testing phase.
B. Data disclosure may occur during the migration event
C. Unexpected outcomes may arise in production
D. Breaches of compliance obligations will occur.

**Correct Answer: C**
**Section:**
**Explanation:**

Unexpected outcomes may arise in production when using only sanitized data for the testing of applications. Sanitized data is data that has been purposely and permanently deleted or modified to prevent unauthorized access or misuse. Sanitized data may not reflect the real characteristics, patterns, or behaviors of the original data, and thus may not be suitable for testing applications that rely on data quality and accuracy. According to NIST, data sanitization methods can affect the usability of data for testing purposes1. The other options are not risks introduced by using sanitized data for testing applications, but rather risks that can be mitigated by using sanitized data. Data loss, data disclosure, and breaches of compliance obligations are possible consequences of using unsanitized data that contains sensitive or confidential information.
Reference: 2: What is Data Sanitization? | Data Erasure Methods | Imperva 3: Data sanitization techniques: Standards, practices, legislation 1: Data sanitization -- Wikipedia

**QUESTION 171**
Which of the following is the BEST method to ensure compliance with password standards?

A. Implementing password-synchronization software
B. Using password-cracking software
C. Automated enforcement of password syntax rules
D. A user-awareness program

**Correct Answer: C**
**Section:**
**Explanation:**
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security. Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards.
Reference: 1: NIST Password Guidelines and Best Practices for 2020 - Auth0 2: Password synchronization - Wikipedia 3:



**QUESTION 172**
Which of the following factors has the GREATEST influence on the successful implementation of information security strategy goals?

A. Regulatory requirements
B. Compliance acceptance
C. Management support
D. Budgetary approval

**Correct Answer: C**
**Section:**
**Explanation:**
Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance1. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with2. Compliance acceptance is the degree to which the organization adheres to the information security policies and standards3. Budgetary approval is the process of allocating financial resources for the information security activities and initiatives4.
Reference: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

**QUESTION 173**
Management has announced the acquisition of a new company. The information security manager of the parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies. To BEST address this concern, the information security manager should:

A. review access rights as the acquisition integration occurs.
B. perform a risk assessment of the access rights.
C. escalate concerns for conflicting access rights to management.
D. implement consistent access control standards.

**Correct Answer: B**
**Section:**
**Explanation:**
Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units.
Reference: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful post-merger integration

**QUESTION 174**
An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance.
Which of the following would provide the MOST useful information for planning purposes?

A. Results from a business impact analysis (BIA)
B. Deadlines and penalties for noncompliance
C. Results from a gap analysis
D. An inventory of security controls currently in place

**Correct Answer: C**
**Section:**
**Explanation:**
Results from a gap analysis would provide the most useful information for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. A gap analysis is an assessment of the difference between an organization's current state of compliance and its desired level or standard. It is a process used to identify potential areas for improvement by comparing actual performance with expected performance. A gap analysis can help to prioritize the actions needed to close the gaps and comply with the regulatory requirements, as well as to estimate the resources and time required for each action1.
The other options are not as useful as results from a gap analysis for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. Deadlines and penalties for noncompliance are important factors to consider, but they do not provide information on how to achieve compliance or what actions are needed2. Results from a business impact analysis (BIA) are useful for identifying the critical processes and assets that need to be protected, but they do not provide information on how to comply with the regulatory requirements or what actions are needed3. An inventory of security controls currently in place is useful for assessing the current state of compliance, but it does not provide information on how to comply with the regulatory requirements or what actions are needed4.
Reference: 3: Business impact analysis (BIA) - Wikipedia 2: Compliance Gap Analysis & Effectiveness Evaluation | SMS 1: What is Gap Analysis in Compliance | Scytale 4: Gap Analysis & Risk Assessment --- Riddle Compliance

**QUESTION 175**
Which of the following documents should contain the INITIAL prioritization of recovery of services?

A. IT risk analysis
B. Threat assessment
C. Business impact analysis (BIA)
D. Business process map

**Correct Answer: C**

**Section:**
**Explanation:**
A business impact analysis (BIA) is the document that should contain the initial priori-tization of recovery of services. A BIA is a process of identifying and analyzing the po-tential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:
* Identifying the critical business functions and processes that support the organization's mission and objectives.
* Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.
* Assessing the potential impacts of disruptions to each function or process, such as finan-cial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatis-faction, etc.
* Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.
* Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.
A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or re-covery of critical business functions and processes in the event of a disruption2. The other options are not documents that should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3. A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes.
Reference: 1: Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process map-ping - Wikipedia

**QUESTION 176**
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.

**Correct Answer: A**
**Section:**
**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.

Reference: 1: Information Classification - Ad-visera 2: Information Classification in Information Security - GeeksforGeeks : Infor-mation Security Policy - NIST : Information Security Classification Framework - Queensland Government

**QUESTION 177**
Which of the following is the GREATEST benefit of information asset classification?

A. Helping to determine the recovery point objective (RPO)
B. Providing a basis for implementing a need-to-know policy
C. Supporting segregation of duties
D. Defining resource ownership

**Correct Answer: B**
**Section:**
**Explanation:**
The greatest benefit of information asset classification is providing a basis for imple-menting a need-to-know policy. Information asset classification is a process of catego-rizing information based on its level of sensitivity and importance, and applying appro-priate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by:
* Defining the value and protection requirements of different types of information
* Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
* Establishing the roles and responsibilities of information owners, custodians, and users
* Enforcing access controls and encryption for the information
* Documenting the security policies and procedures for the information
By providing a basis for implementing a need-to-know policy, information asset classi-fication can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification. Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud4. De-fining resource ownership is not a benefit, but rather a component of information asset classification. Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5.
Reference: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3: Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST : Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy - UCI

**QUESTION 178**
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?

A. The benefit is greater than the potential risk.
B. USB storage devices are enabled based on user roles.
C. Users accept the risk of noncompliance.
D. Access is restricted to read-only.

**Correct Answer: A**
**Section:**
**Explanation:**
The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security pol-icy should also be aligned with the organization's business objectives and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2. The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected

to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as:
* Enhancing data mobility and accessibility
* Improving data backup and recovery
* Supporting data sharing and collaboration
* Enabling data encryption and authentication
However, USB storage devices also pose significant security risks for users and organi-zations, such as:
* Introducing malware or viruses to laptops and desktops
* Exposing sensitive data to unauthorized access or disclosure
* Losing or stealing data due to device loss or theft
* Violating security policies or regulations
Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4. Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5.
Reference: 1: Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

**QUESTION 179**
What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

A. Determine operational losses.
B. Improve the change control process.
C. Update the threat landscape.
D. Review the effectiveness of controls

**Correct Answer: D**
**Section:**
**Explanation:**
The primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. A business system update is a process of modifying or enhancing an information system to improve its functionality, performance, security, or compatibility. A business system update may introduce new features, fix bugs, patch vulnerabilities, or comply with new standards or regulations2. Performing a vulnerability assessment following a business system update is important because it helps to:
* Review the effectiveness of controls that are implemented to protect the information sys-tem from threats and risks
* Identify any new or residual vulnerabilities that may have been introduced or exposed by the update
* Evaluate the impact and likelihood of potential incidents that may exploit the vulnerabili-ties
* Prioritize and implement appropriate actions to address the vulnerabilities
* Verify and validate the security posture and compliance of the updated information sys-tem
Therefore, the primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls that are designed to ensure the confidentiality, integrity, and availability of the information system and its dat
a. The other options are not the primary objectives of performing a vulnerability as-sessment following a business system update. Determining operational losses is not an objective, but rather a possible consequence of not performing a vulnerability as-sessment or not addressing the identified vulnerabilities. Improving the change control process is not an objective, but rather a possible outcome of performing a vulnerability assessment and incorporating its results and recommendations into the change man-agement cycle. Updating the threat landscape is not an objective, but rather a prereq-uisite for performing a vulnerability assessment that requires using up-to-date sources of threat intelligence and vulnerability information.
Reference: 1: Vulnerability As-sessment - NIST 2: System Update - Techopedia : Vulnerability Assessment vs Penetra-tion Testing - Imperva : Change Control Process - NIST : Threat Landscape - NIST

**QUESTION 180**

Threat and vulnerability assessments are important PRIMARILY because they are:

A. used to establish security investments
B. the basis for setting control objectives.
C. elements of the organization's security posture.
D. needed to estimate risk.

**Correct Answer: B**
**Section:**
**Explanation:**
Threat and vulnerability assessments are important PRIMARILY because they are the basis for setting control objectives. Control objectives are the desired outcomes or goals of implementing security controls in an information system. They are derived from the risk assessment process, which identifies and evaluates the threats and vulnerabilities that could affect the system's confidentiality, integrity and availability. By conducting threat and vulnerability assessments, an organization can determine the level of risk it faces and establish the appropriate control objectives to mitigate those risks.

**QUESTION 181**
An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?

A. Identify the skill set of the provider's incident response team.
B. Evaluate the provider's audit logging and monitoring controls.
C. Review the provider's incident definitions and notification criteria.
D. Update the incident escalation process.

**Correct Answer: D**
**Section:**
**Explanation:**
Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.
Topic 3, Exam Pool C

**QUESTION 182**
Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?

A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes
C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards

**Correct Answer: D**
**Section:**
**Explanation:**
An independent review report indicating compliance with industry standards BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

**QUESTION 183**
Which of the following should be the FIRST step in developing an information security strategy?

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

**Correct Answer: A**
**Section:**
**Explanation:**
first step in developing an information security strategy is to conduct a risk-aware and comprehensive inventory of your company's context, including all digital assets, employees, and vendors. Then you need to know about the threat environment and which types of attacks are a threat to your company1. This is similar to performing a gap analysis based on the current state3.

**QUESTION 184**
To help ensure that an information security training program is MOST effective, its contents should be:

A. based on recent incidents.
B. based on employees' roles.
C. aligned to business processes.
D. focused on information security policy.

**Correct Answer: B**
**Section:**
**Explanation:**
To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles. This is because different roles have different responsibilities and access levels to information and systems, and therefore face different types of threats and risks. By tailoring the training content to the specific needs and expectations of each role, the training program can increase the relevance and retention of the information security knowledge and skills for the employees. Role-based training can also help employees understand their accountability and obligations for protecting information assets in their daily tasks

**QUESTION 185**
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.

**Correct Answer: C**
**Section:**
**Explanation:**
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

**QUESTION 186**
Which of the following is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business?

A. Risk assessment program
B. Information security awareness training
C. Information security governance

D. Information security metrics

**Correct Answer: C**
**Section:**
**Explanation:**
Information security governance is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business. This is because information security governance provides the strategic direction, oversight and accountability for the cybersecurity program. It also ensures that the program aligns with the business objectives, risk appetite and compliance requirements of the organization. Information security governance involves defining roles and responsibilities, establishing policies and standards, setting goals and metrics, allocating resources and monitoring performance of the cybersecurity program.

**QUESTION 187**
Which of the following provides the MOST comprehensive insight into ongoing threats facing an organization?

A. Business impact analysis (BIA)
B. Risk register
C. Penetration testing
D. Vulnerability assessment

**Correct Answer: B**
**Section:**
**Explanation:**
A risk register provides the MOST comprehensive insight into ongoing threats facing an organization. This is because a risk register is a document that records and tracks the identified risks, their likelihood, impact, mitigation strategies, and status. A risk register helps an organization to monitor and manage the threats that could affect its objectives, assets, and operations. A risk register also helps an organization to prioritize its response efforts and allocate its resources accordingly.

**QUESTION 188**
An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

A. Set up communication channels for the target audience.
B. Determine the needs and requirements of each audience.
C. Create a comprehensive singular communication
D. Invoke the organization's incident response plan.

**Correct Answer: B**
**Section:**
**Explanation:**
Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

**QUESTION 189**
Which of the following would be MOST useful to help senior management understand the status of information security compliance?

A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Business impact analysis (BIA) results
D. Risk assessment results

**Correct Answer: B**
**Section:**
**Explanation:**
Key performance indicators (KPIs) are metrics that measure the effectiveness and ef-ficiency of information security processes and activities. They help senior manage-ment understand the status of information security compliance by providing relevant, timely and accurate information on the performance of security controls, the level of risk exposure, the return on security investment and the progress toward security ob-jectives. KPIs can also be used to benchmark the organization's security performance against industry standards or best practices. KPIs should be aligned with the organiza-tion's strategic goals and risk appetite, and should be reported regularly to senior man-agement and other stakeholders.
* 1 Key Performance Indicators for Security Governance, Part 1 - ISACA
* 2 Key Performance Indicators for Security Governance, Part 2 - ISACA
* 3 Compliance Metrics and KPIs For Measuring Compliance Effectiveness - Reciprocity
* 4 14 Cybersecurity Metrics + KPIs You Must Track in 2023 - UpGuard

**QUESTION 190**
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

A. service level agreements (SLAs)
B. security requirements for the process being outsourced.
C. risk-reporting methodologies.
D. security metrics

**Correct Answer: B**
**Section:**
**Explanation:**
Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information. They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are essential to protect the information assets of the organization and to establish a clear and en-forceable contractual relationship with the third party.
* 1 Outsourcing Strategies for Information Security: Correlated Losses and Security Exter-nalities - SpringerLink
* 2 What requirements must outsourcing services comply with for the European market? - CBI
* 3 Outsourcing cybersecurity: What services to outsource, what to keep in house - Infosec Institute
* 4 BCFSA outsourcing and information security guidelines - BLG

**QUESTION 191**
Which of the following is the GREATEST concern resulting from the lack of severity criteria in incident classification?

A. Statistical reports will be incorrect.
B. The service desk will be staffed incorrectly.
C. Escalation procedures will be ineffective.
D. Timely detection of attacks will be impossible.

**Correct Answer: C**
**Section:**
**Explanation:**
The greatest concern resulting from the lack of severity criteria in incident classification is that escalation procedures will be ineffective because they rely on severity criteria to determine when and how to escalate an incident to higher levels of authority or responsibility, and what actions or resources are required for resolving an incident. Statistical reports will be incorrect is not a great concern because they do not affect the incident response process directly, but rather provide information or analysis for improvement or evaluation purposes. The service desk will be staffed incorrectly is not a great concern because it does not affect the incident response process directly, but rather affects the availability or efficiency of one of its components. Timely detection of attacks will be impossible is not a great concern because it does not depend on severity criteria, but rather on monitoring and alerting mechanisms.

Reference: 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

**QUESTION 192**
In a call center, the BEST reason to conduct a social engineering is to:

A. Identify candidates for additional security training.
B. minimize the likelihood of successful attacks.
C. gain funding for information security initiatives.
D. improve password policy.

**Correct Answer: A**
**Section:**
**Explanation:**
The best reason to conduct a social engineering test in a call center is to identify candidates for additional security training because it helps to assess the level of awareness and skills of the call center staff in recognizing and resisting social engineering attacks, and provide them with the necessary training or education to improve their security posture. Minimizing the likelihood of successful attacks is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Gaining funding for information security initiatives is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Improving password policy is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

**QUESTION 193**
Which of the following should include contact information for representatives of equipment and software vendors?

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

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

**QUESTION 194**
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

**Correct Answer: A**
**Section:**
**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.
Reference: 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

**QUESTION 195**
The contribution of recovery point objective (RPO) to disaster recovery is to:

A. minimize outage periods.
B. eliminate single points of failure.
C. define backup strategy
D. reduce mean time between failures (MTBF).

**Correct Answer: C**
**Section:**
**Explanation:**
The contribution of recovery point objective (RPO) to disaster recovery is to define backup strategy because it determines the maximum amount of data loss that is acceptable to an organization after a disruption, and guides the frequency and type of backups needed to restore the data to a usable format1.Minimize outage periods is not a contribution of RPO, but rather a contribution of recovery time objective (RTO), which defines the maximum amount of time that is acceptable to restore normal operations after a disruption2.Eliminate single points of failure is not a contribution of RPO, but rather a goal of high availability (HA), which ensures that systems or services are continuously operational and resilient3.Reduce mean time between failures (MTBF) is not a contribution of RPO, but rather a measure of reliability, which indicates the average time that a system or component operates without failure4.
Reference:1https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs2https://www.druva.com/glossary/what-is-a-recovery-time-objective-definition-and-related-faqs3https://www.fortinet.com/resources/cyberglossary/high-availability4https://www.fortinet.com/resources/cyberglossary/mean-time-between-failures

**QUESTION 196**
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.

**Correct Answer: B**
**Section:**
**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.
Reference: 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

**QUESTION 197**
The PRIMARY goal of the eradication phase in an incident response process is to:

A. maintain a strict chain of custody.
B. provide effective triage and containment of the incident.
C. remove the threat and restore affected systems
D. obtain forensic evidence from the affected system.

**Correct Answer: C**
**Section:**
**Explanation:**
The primary goal of the eradication phase in an incident response process is to remove the threat and restore affected systems because it eliminates any traces or remnants of malicious activity or compromise from the systems or network, and returns them to their normal or secure state. Maintaining a strict chain of custody is not a goal of the eradication phase, but rather a requirement for preserving and documenting digital evidence throughout the incident response process. Providing effective triage and containment of the incident is not a goal of the eradication phase, but rather a goal of the containment phase, which isolates and stops the spread of malicious activity or compromise. Obtaining forensic evidence from the affected system is not a goal of the eradication phase, but rather a goal of the identification phase, which collects and analyzes data or artifacts related to malicious activity or compromise.
Reference: 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

**QUESTION 198**
An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:
* A bad actor broke into a business-critical FTP server by brute forcing an administrative password
* The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
* The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
* After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail
Which of the following could have been prevented by conducting regular incident response testing?

A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data

**Correct Answer: A**
**Section:**
**Explanation:**
Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process.
Reference: 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

**QUESTION 199**
Which of the following is the BEST option to lower the cost to implement application security controls?

A. Perform security tests in the development environment.
B. Integrate security activities within the development process

C. Perform a risk analysis after project completion.
D. Include standard application security requirements

**Correct Answer: B**
**Section:**
**Explanation:**
Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios. Performing a risk analysis after project completion is not a good option because it may be too late to identify or mitigate security risks that may have been introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems

**QUESTION 200**
Which of the following would provide the MOST effective security outcome in an organizations contract management process?

A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage
B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage
C. Extending security assessment to cover asset disposal on contract termination
D. Extending security assessment to include random penetration testing

**Correct Answer: B**
**Section:**
**Explanation:**
Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance. Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

**QUESTION 201**
A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?

A. Determine the required security controls for the new solution
B. Review the disaster recovery plans (DRPs) of the providers
C. Obtain audit reports on the service providers' hosting environment
D. Align the roles of the organization's and the service providers' stats.

**Correct Answer: A**
**Section:**
**Explanation:**
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements.

Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

**QUESTION 202**
Which of the following is the BEST way lo monitor for advanced persistent threats (APT) in an organization?

A. Network with peers in the industry to share information.
B. Browse the Internet to team of potential events
C. Search for anomalies in the environment
D. Search for threat signatures in the environment.

**Correct Answer: C**
**Section:**
**Explanation:**
An advanced persistent threat (APT) is a stealthy and sophisticated attack that aims to compromise and maintain access to a target network or system over a long period of time, often for espionage or sabotage purposes. APTs are difficult to detect by conventional security tools, such as antivirus or firewalls, that rely on signatures or rules to identify threats. Therefore, the best way to monitor for APTs is to search for anomalies in the environment, such as unusual network traffic, user behavior, file activity, or system configuration changes, that may indicate a compromise or an ongoing attack.
Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

**QUESTION 203**
Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?

A. Conduct a cost-benefit analysis.
B. Consult corporate legal counsel
C. Update the information security policy.
D. Perform a gap analysis.

**Correct Answer: D**
**Section:**
**Explanation:**
When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements.
Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

**QUESTION 204**
In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?

A. Ownership of security
B. Compliance with policies
C. Auditability of systems
D. Allocation of training resources

**Correct Answer: A**
**Section:**
**Explanation:**
Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws

and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks.
Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

**QUESTION 205**
An organization is leveraging tablets to replace desktop computers shared by shift-based staff These tablets contain critical business data and are inherently at increased risk of theft Which of the following will BEST help to mitigate this risk''

A. Deploy mobile device management (MDM)
B. Implement remote wipe capability.
C. Create an acceptable use policy.
D. Conduct a mobile device risk assessment

**Correct Answer: D**
**Section:**
**Explanation:**
A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones.
Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

**QUESTION 206**
Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

A. Return on investment (ROI)
B. Compliance requirements
C. Target audience
D. Criticality of information

**Correct Answer: D**
**Section:**
**Explanation:**
A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones.
Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

**QUESTION 207**
Which of the following BEST enables an organization to effectively manage emerging cyber risk?

A. Periodic internal and external audits
B. Clear lines of responsibility
C. Sufficient cyber budget allocation
D. Cybersecurity policies

**Correct Answer: D**

**Section:**
**Explanation:**
Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals.
Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

**QUESTION 208**
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

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

**Correct Answer: B**
**Section:**

**QUESTION 209**
An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

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

**Correct Answer: A**
**Section:**

**QUESTION 210**
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.

**Correct Answer: D**
**Section:**

**QUESTION 211**
Which of the following is the BEST way to address data availability concerns when outsourcing information security administration?

A. Develop service level agreements (SLAs).

B. Stipulate insurance requirements.
C. Require nondisclosure agreements (NDAs).
D. Create contingency plans.

**Correct Answer: D**
**Section:**

**QUESTION 212**
What should be the FIRST step when implementing data loss prevention (DLP) technology?

A. Perform due diligence with vendor candidates.
B. Build a business case.
C. Classify the organization's data.
D. Perform a cost-benefit analysis.

**Correct Answer: C**
**Section:**

**QUESTION 213**
In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?

A. Access to the hardware
B. Data encryption
C. Non-standard event logs
D. Compressed customer data

**Correct Answer: C**
**Section:**

**QUESTION 214**
Which of the following would provide the MOST value to senior management when presenting the results of a risk assessment?

A. Mapping the risks to the security classification scheme
B. Illustrating risk on a heat map
C. Mapping the risks to existing controls
D. Providing a technical risk assessment report

**Correct Answer: B**
**Section:**

**QUESTION 215**
Identifying which of the following BEST enables a cyberattack to be contained?

A. The vulnerability exploited by the attack
B. The segment targeted by the attack
C. The IP address of the computer that launched the attack
D. The threat actor that initiated the attack

**Correct Answer: B**
**Section:**

**QUESTION 216**
To ensure that a new application complies with information security policy, the BEST approach is to:

A. review the security of the application before implementation.
B. integrate functionality the development stage.
C. perform a vulnerability analysis.
D. periodically audit the security of the application.

**Correct Answer: C**
**Section:**
**Explanation:**
Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

**QUESTION 217**
An information security manager has identified that security risks are not being treated in a timely manner. Which of the following

A. Provide regular updates about the current state of the risks.
B. Re-perform risk analysis at regular intervals.
C. Assign a risk owner to each risk
D. Create mitigating controls to manage the risks.

**Correct Answer: B**
**Section:**
**Explanation:**
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content.
Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com/searchsecurity/definition/digital-signature

**QUESTION 218**
An email digital signature will:

A. protect the confidentiality of an email message.
B. verify to recipient the integrity of an email message.
C. automatically correct unauthorized modification of an email message.
D. prevent unauthorized modification of an email message.

**Correct Answer: B**

**Section:**
**Explanation:**
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content.
Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com/searchsecurity/definition/digital-signature

**QUESTION 219**
From an information security perspective, legal issues associated with a transborder flow of technology-related items are MOST often

A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.

**Correct Answer: C**
**Section:**
**Explanation:**
Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow.
Reference: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on-transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

**QUESTION 220**
Which of the following BEST supports effective communication during information security incidents7

A. Frequent incident response training sessions
B. Centralized control monitoring capabilities
C. Responsibilities defined within role descriptions
D. Predetermined service level agreements (SLAs)

**Correct Answer: D**
**Section:**
**Explanation:**
The best way to support effective communication during information security incidents is to have predetermined service level agreements (SLAs) because they define the expectations and responsibilities of the parties involved in the incident response process, and specify the communication channels, methods, and frequency for reporting and updating on the incident status and resolution. Frequent incident response training sessions are not very effective because they do not address the communication needs or challenges during an actual incident. Centralized control monitoring capabilities are not very effective because they do not address the communication needs or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or challenges during an actual incident.
Reference: 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

**QUESTION 221**
After a recovery from a successful malware attack, instances of the malware continue to be discovered. Which phase of incident response was not successful?

A. Eradication
B. Recovery
C. Lessons learned review
D. Incident declaration

**Correct Answer: A**
**Section:**
**Explanation:**
Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.
https://www.securitymetrics.com/blog/6-phases-incident-response-plan
https://www.atlassian.com/incident-management/incident-response
https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

**QUESTION 222**
An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?

A. Security requirements are included in the vendor contract
B. External security audit results are reviewed.
C. Service level agreements (SLAs) meet operational standards.
D. Business continuity contingency planning is provided

**Correct Answer: A**
**Section:**
**Explanation:**
Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.
https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations
https://www.sciencedirect.com/science/article/pii/S0378720616302166

**QUESTION 223**
A penetration test against an organization's external web application shows several vulnerabilities. Which of the following presents the GREATEST concern?

A. A rules of engagement form was not signed prior to the penetration test
B. Vulnerabilities were not found by internal tests
C. Vulnerabilities were caused by insufficient user acceptance testing (UAT)
D. Exploit code for one of the vulnerabilities is publicly available

**Correct Answer: D**
**Section:**
**Explanation:**
Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.
https://www.imperva.com/learn/application-security/penetration-testing/
https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web-application-for-vulnerabilities/

**QUESTION 224**
Which of the following is MOST helpful in determining the criticality of an organization's business functions?

A. Disaster recovery plan (DRP)
B. Business impact analysis (BIA)
C. Business continuity plan (BCP)
D. Security assessment report (SAR)

**Correct Answer: B**
**Section:**
**Explanation:**
Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.
https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez
https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business-continuity-Understanding-impact-criticality

**QUESTION 225**
An organization has purchased an Internet sales company to extend the sales department. The information security manager's FIRST step to ensure the security policy framework encompasses the new business model is to:

A. perform a gap analysis.
B. implement both companies' policies separately
C. merge both companies' policies
D. perform a vulnerability assessment

**Correct Answer: A**
**Section:**
**Explanation:**
Performing a gap analysis is the first step to ensure the security policy framework encompasses the new business model because it is a process of comparing the current state of security policies and controls with the desired or required state. A gap analysis helps to identify the strengths and weaknesses of the existing security policy framework, as well as the opportunities and threats posed by the new business model. A gap analysis also helps to prioritize the actions and resources needed to close the gaps and align the security policy framework with the new business objectives and requirements. Therefore, performing a gap analysis is the correct answer.
https://secureframe.com/blog/security-frameworks
https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

**QUESTION 226**
A forensic examination of a PC is required, but the PC has been switched off. Which of the following should be done FIRST?

A. Perform a backup of the hard drive using backup utilities.
B. Perform a bit-by-bit backup of the hard disk using a write-blocking device
C. Perform a backup of the computer using the network
D. Reboot the system using third-party forensic software in the CD-ROM drive

**Correct Answer: B**
**Section:**
**Explanation:**
Performing a bit-by-bit backup of the hard disk using a write-blocking device is the first step to do when a forensic examination of a PC is required, but the PC has been switched off because it helps to create a forensically sound copy of the original evidence without altering or damaging it. A bit-by-bit backup, also known as a physical or raw image, is a complete copy of every bit on the hard disk, including the unallocated or deleted data. A write-blocking device is a hardware or software tool that prevents any write operations to the hard disk, such as updating timestamps or changing file attributes. Performing a bit-by-bit backup of the hard disk using a write-blocking device ensures the integrity and authenticity of the evidence and allows the forensic analysis to be conducted on the duplicate image rather than the original source. Therefore, performing a bit-by-bit backup of the

hard disk using a write-blocking device is the correct answer.
https://en.wikipedia.org/wiki/Computer_forensics
https://resources.infosecinstitute.com/topic/computer-forensics-forensic-analysis-examination-planning/
https://www.computer-forensics-recruiter.com/topics/examination_steps/

**QUESTION 227**
Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?

A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider

**Correct Answer: D**
**Section:**
**Explanation:**
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider.
Reference:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a-long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117-p599mr

**QUESTION 228**
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

**Correct Answer: D**
**Section:**
**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.
Reference:
https://www.iso.org/standard/74046.html
https://www.nist.gov/cyberframework
https://www.iso.org/standard/27001

**QUESTION 229**
An incident response team has established that an application has been breached. Which of the following should be done NEXT?

A. Maintain the affected systems in a forensically acceptable state

B. Conduct a risk assessment on the affected application
C. Inform senior management of the breach.
D. Isolate the impacted systems from the rest of the network

**Correct Answer: D**
**Section:**
**Explanation:**
The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems.
Reference:
https://www.crowdstrike.com/cybersecurity-101/incident-response/
https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks
https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security/

**QUESTION 230**
An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

A. Lack of availability
B. Lack of accountability
C. Improper authorization
D. Inadequate authentication

**Correct Answer: B**
**Section:**
**Explanation:**
The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions.
Reference:
https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam
https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices
https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

**QUESTION 231**
Which of the following is the MOST effective way to detect information security incidents?

A. Implementation of regular security awareness programs
B. Periodic analysis of security event log records
C. Threshold settings on key risk indicators (KRIs)
D. Real-time monitoring of network activity

**Correct Answer: D**
**Section:**

**QUESTION 232**
Which of the following is MOST important to include in an information security policy?

A. Best practices
B. Management objectives
C. Baselines
D. Maturity levels

**Correct Answer: B**
**Section:**

**QUESTION 233**
When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure:

A. the integrity of evidence is preserved.
B. forensic investigation software is loaded on the server.
C. the incident is reported to senior management.
D. the server is unplugged from power.

**Correct Answer: A**
**Section:**

**QUESTION 234**
Which or the following is MOST important to consider when determining backup frequency?

A. Recovery point objective (RPO)
B. Recovery time objective (RTO)
C. Allowable interruption window
D. Maximum tolerable outage (MTO)

**Correct Answer: A**
**Section:**

**QUESTION 235**
Which of the following should be done FIRST when a SIEM flags a potential event?

A. Validate the event is not a false positive.
B. Initiate the incident response plan.
C. Escalate the event to the business owner.
D. Implement compensating controls.

**Correct Answer: A**
**Section:**
**Explanation:**
The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls. Validation can be done by analyzing the event data, comparing it with the baseline or normal

behavior, and checking for any anomalies or indicators of compromise.
A false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 72, page 19

**QUESTION 236**
Which of the following should an information security manager do NEXT after creating a roadmap to execute the strategy for an information security program?

A. Obtain consensus on the strategy from the executive board.
B. Review alignment with business goals.
C. Define organizational risk tolerance.
D. Develop a project plan to implement the strategy.

**Correct Answer: D**
**Section:**
**Explanation:**
The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors.
A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

**QUESTION 237**
Which of the following is the MOST effective way to determine the alignment of an information security program with the business strategy?

A. Evaluate the results of business continuity testing.
B. Review key performance indicators (KPIs).
C. Evaluate the business impact of incidents.
D. Engage business process owners.

**Correct Answer: D**
**Section:**
**Explanation:**
The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.
Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20