CISM.exam.400q

Number: CISM
Passing Score: 800
Time Limit: 120 min

CISM

Certified Information Security Manager

Sections

1. INFORMATION SECURITY GOVERNANCE
2. INFORMATION RISK MANAGEMENT
3. INFORMATION SECURITY PROGRAM DEVELOPMENT
4. INFORMATION SECURITY PROGRAM MANAGEMENT

5. INCIDENT MANAGEMENT AND RESPONSE

Exam A

QUESTION 1
Who is ultimately responsible for the organization's information?

A. Data custodian
B. Chief information security officer (CISO)
C. Board of directors
D. Chief information officer (CIO)

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The board of directors is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. The data custodian is responsible for the maintenance and protection of data. This role is usually filled by the IT department. The chief information security officer (CISO) is responsible for security and carrying out senior management's directives. The chief information officer (CIO) is responsible for information technology within the organization and is not ultimately responsible for the organization's information.

QUESTION 2
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

A. Alignment with industry best practices
B. Business continuity investment

C. Business benefits
D. Regulatory compliance

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

Regulatory compliance can be a standalone driver for an information security governance measure. No further analysis nor justification is required since the entity has no choice in the regulatory requirements. Buy-in from business managers must be obtained by the information security manager when an information security governance measure is sought based on its alignment with industry best practices. Business continuity investment needs to be justified by business impact analysis. When an information security governance measure is sought based on qualitative business benefits, further analysis is required to determine whether the benefits outweigh the cost of the information security governance measure in question.

QUESTION 3
A security manager meeting the requirements for the international flow of personal data will need to ensure:

A. a data processing agreement.
B. a data protection registration.
C. the agreement of the data subjects.
D. subject access procedures.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Whenever personal data are transferred across national boundaries, the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

QUESTION 4
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

A. Ethics

B. Proportionality
C. Integration
D. Accountability

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules (types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

QUESTION 5
Which of the following is the MOST important prerequisite for establishing information security management within an organization?

A. Senior management commitment
B. Information security framework
C. Information security organizational structure
D. Information security policy

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Senior management commitment is necessary in order for each of the other elements to succeed. Without senior management commitment, the other elements will likely be ignored within the organization.

QUESTION 6
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees
B. Distance between physical locations

C. Complexity of organizational structure
D. Organizational budget

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance. Organizational budget is not a major impact once good governance models are in place; hence governance will help in effective management of the organization's budget.

QUESTION 7
In order to highlight to management, the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

A. prepare a security budget.
B. conduct a risk assessment.
C. develop an information security policy.
D. obtain benchmarking information.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Risk assessment, evaluation and impact analysis will be the starting point for driving management's attention to information security. All other choices will follow the risk assessment.

QUESTION 8
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

A. it implies compliance risks.
B. short-term impact cannot be determined.
C. it violates industry security practices.
D. changes in the roles matrix cannot be detected.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

QUESTION 9
An outcome of effective security governance is:

A. business dependency assessment
B. strategic alignment.
C. risk assessment.
D. planning.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Business dependency assessment is a process of determining the dependency of a business on certain information resources. It is not an outcome or a product of effective security management. Strategic alignment is an outcome of effective security governance. Where there is good governance, there is likely to be strategic alignment. Risk assessment is not an outcome of effective security governance; it is a process. Planning comes at the beginning of effective security governance, and is not an outcome but a process.

QUESTION 10
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

A. Give organization standards preference over local regulations
B. Follow local regulations only
C. Make the organization aware of those standards where local regulations causes conflicts
D. Negotiate a local version of the organization standards

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Adherence to local regulations must always be the priority. Not following local regulations can prove detrimental to the group organization. Following local regulations only is incorrect since there needs to be some recognition of organization requirements. Making an organization aware of standards is a sensible step, but is not a total solution. Negotiating a local version of the organization standards is the most effective compromise in this situation.

QUESTION 11
Who should drive the risk analysis for an organization?

A. Senior management
B. Security managerC. Quality manager
D. Legal department

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Although senior management should support and sponsor a risk analysis, the know-how and the management of the project will be with the security department. Quality management and the legal department will contribute to the project.

QUESTION 12
The FIRST step in developing an information security management program is to:

A. identify business risks that affect the organization.
B. clarify organizational purpose for creating the program.
C. assign responsibility for the program.
D. assess adequacy of controls to mitigate business risks.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

In developing an information security management program, the first step is to clarify the organization's purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

QUESTION 13
Which of the following is the MOST important to keep in mind when assessing the value of information?

A. The potential financial loss
B. The cost of recreating the information
C. The cost of insurance coverage
D. Regulatory requirement

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The potential for financial loss is always a key factor when assessing the value of information. Choices B, C and D may be contributors, but not the key factor.

QUESTION 14
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

A. Risk assessment report
B. Technical evaluation report
C. Business case
D. Budgetary requirements

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

The information security manager needs to prioritize the controls based on risk management and the requirements of the organization. The information security manager must look at the costs of the various controls and compare them against the benefit the organization will receive from the security solution. The information security manager needs to have knowledge of the development of business cases to illustrate the costs and benefits of the various controls. All other choices are supplemental.

QUESTION 15
To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

A. Security breach frequency
B. Annualized loss expectancy (ALE)
C. Cost-benefit analysis
D. Peer group comparison

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Cost-benefit analysis is the legitimate way to justify budget. The frequency of security breaches may assist the argument for budget but is not the key tool; it does not address the impact. Annualized loss expectancy (ALE) does not address the potential benefit of security investment. Peer group comparison would provide a good estimate for the necessary security budget but it would not take into account the specific needs of the organization.

QUESTION 16
Which of the following situations would MOST inhibit the effective implementation of security governance?

A. The complexity of technology B.
Budgetary constraints
C. Conflicting business priorities
D. High-level sponsorship

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

The need for senior management involvement and support is a key success factor for the implementation of appropriate security governance. Complexity of technology, budgetary constraints and conflicting business priorities are realities that should be factored into the governance model of the organization, and should not be regarded as inhibitors.

QUESTION 17
To achieve effective strategic alignment of security initiatives, it is important that:

A. Steering committee leadership be selected by rotation.
B. Inputs be obtained and consensus achieved between the major organizational units.
C. The business strategy be updated periodically.
D. Procedures and standards be approved by all departmental heads.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

It is important to achieve consensus on risks and controls, and obtain inputs from various organizational entities since security needs to be aligned to the needs of the organization. Rotation of steering committee leadership does not help in achieving strategic alignment. Updating business strategy does not lead to strategic alignment of security initiatives. Procedures and standards need not be approved by all departmental heads

QUESTION 18
What would be the MOST significant security risks when using wireless local area network (LAN) technology?

A. Man-in-the-middle attack
B. Spoofing of data packets
C. Rogue access point
D. Session hijacking

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
A rogue access point masquerades as a legitimate access point The risk is that legitimate users may connect through this access point and have their traffic monitored. All other choices are not dependent on the use of a wireless local area network (LAN) technology.

QUESTION 19
When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

A. Business management
B. Operations manager
C. Information security manager
D. System users

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

QUESTION 20
In implementing information security governance, the information security manager is PRIMARILY responsible for:

A. developing the security strategy.
B. reviewing the security strategy.
C. communicating the security strategy.
D. approving the security strategy

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

QUESTION 21
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

A. performance measurement.
B. integration.
C. alignment.
D. value delivery.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Strategic alignment of security with business objectives is a key indicator of performance measurement. In guiding a security program, a meaningful performance measurement will also rely on an understanding of business objectives, which will be an outcome of alignment. Business linkages do not by themselves indicate integration or value delivery. While alignment is an important precondition, it is not as important an indicator.

QUESTION 22

When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

A. Compliance with international security standards.
B. Use of a two-factor authentication system.
C. Existence of an alternate hot site in case of business disruption.
D. Compliance with the organization's information security requirements.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Prom a security standpoint, compliance with the organization's information security requirements is one of the most important topics that should be included in the contract with third-party service provider. The scope of implemented controls in any ISO 27001-compliant organization depends on the security requirements established by each organization. Requiring compliance only with this security standard does not guarantee that a service provider complies with the organization's security requirements. The requirement to use a specific kind of control methodology is not usually stated in the contract with third- party service providers.

QUESTION 23
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

A. review the functionalities and implementation requirements of the solution.
B. review comparison reports of tool implementation in peer companies.
C. provide examples of situations where such a tool would be useful.
D. substantiate the investment in meeting organizational needs.

Correct Answer: D

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Any investment must be reviewed to determine whether it is cost effective and supports the organizational strategy. It is important to review the features and functionalities provided by such a tool, and to provide examples of situations where the tool would be useful, but that comes after substantiating the investment and return on investment to the organization.

QUESTION 24
The MOST useful way to describe the objectives in the information security strategy is through:

A. attributes and characteristics of the 'desired state."
B. overall control objectives of the security program.
C. mapping the IT systems to key business processes.
D. calculation of annual loss expectations.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

Security strategy will typically cover a wide variety of issues, processes, technologies and outcomes that can best be described by a set of characteristics and attributes that are desired. Control objectives are developed after strategy and policy development. Mapping IT systems to key business processes does not address strategy issues. Calculation of annual loss expectations would not describe the objectives in the information security strategy.

QUESTION 25
In order to highlight to management, the importance of network security, the security manager should FIRST:

A. develop a security architecture.
B. install a network intrusion detection system (NIDS) and prepare a list of attacks.
C. develop a network security policy.
D. conduct a risk assessment.

Correct Answer: D

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

QUESTION 26
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions
C. Organization chart
D. Skills inventory

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
A skills inventory would help identify- the available resources, any gaps and the training requirements for developing resources. Proficiency testing is useful but only with regard to specific technical skills. Job descriptions would not be as useful since they may be out of date or not sufficiently detailed. An organization chart would not provide the details necessary to determine the resources required for this activity.

QUESTION 27
The MOST important characteristic of good security policies is that they:

A. state expectations of IT management.
B. state only one general security mandate.
C. are aligned with organizational goals.
D. govern the creation of procedures and guidelines.

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The most important characteristic of good security policies is that they be aligned with organizational goals. Failure to align policies and goals significantly reduces the value provided by the policies. Stating expectations of IT management omits addressing overall organizational goals and objectives. Stating only one general security mandate is the next best option since policies should be clear; otherwise, policies may be confusing and difficult to understand. Governing the creation of procedures and guidelines is most relevant to information security standards.

QUESTION 28
An information security manager must understand the relationship between information security and business operations in order to:

A. support organizational objectives.
B. determine likely areas of noncompliance.
C. assess the possible impacts of compromise.
D. understand the threats to the business.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Security exists to provide a level of predictability for operations, support for the activities of the organization and to ensure preservation of the organization. Business operations must be the driver for security activities in order to set meaningful objectives, determine and manage the risks to those activities, and provide a basis to measure the effectiveness of and provide guidance to the security program. Regulatory compliance may or may not be an organizational requirement. If compliance is a requirement, some level of compliance must be supported but compliance is only one aspect. It is necessary to understand the business goals in order to assess potential impacts and evaluate threats. These are some of the ways in which security supports organizational objectives, but they are not the only ways.

QUESTION 29
Investment in security technology and processes should be based on:

A. clear alignment with the goals and objectives of the organization.
B. success cases that have been experienced in previous projects.
C. best business practices.

D. safeguards that are inherent in existing technology.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Organization maturity level for the protection of information is a clear alignment with goals and objectives of the organization. Experience in previous projects is dependent upon other business models which may not be applicable to the current model. Best business practices may not be applicable to the organization's business needs. Safeguards inherent to existing technology are low cost but may not address all business needs and/or goals of the organization.

QUESTION 30
The data access requirements for an application should be determined by the:

A. legal department.
B. compliance officer.
C. information security manager.
D. business owner.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Business owners are ultimately responsible for their applications. The legal department, compliance officer and information security manager all can advise, but do not have final responsibility.

QUESTION 31
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. analyzed under the retention policy.
B. protected under the information classification policy.
C. analyzed under the backup policy.
D. protected under the business impact analysis (BIA).

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Option A is the type of analysis that will determine whether the organization is required to maintain the data for business, legal or regulatory reasons. Keeping data that are no longer required unnecessarily consumes resources, and, in the case of sensitive personal information, can increase the risk of data compromise. Options B. C and D are attributes that should be considered in the destruction and retention policy. A BIA could help determine that this information does not support the main objective of the business, but does not indicate the action to take.

QUESTION 32
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

A. Laws and regulations of the country of origin may not be enforceable in the foreign country.
B. A security breach notification might get delayed due to the time difference.
C. Additional network intrusion detection sensors should be installed, resulting in an additional cost.
D. The company could lose physical control over the server and be unable to monitor the physical security posture of the servers.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A company is held to the local laws and regulations of the country in which the company resides, even if the company decides to place servers with a vendor that hosts the servers in a foreign country. A potential violation of local laws applicable to the company might not be recognized or rectified (i.e., prosecuted) due to the lack of knowledge of the local laws that are applicable and the inability to enforce the laws. Option B is not a problem. Time difference does not play a role in a 24/7 environment. Pagers, cellular phones, telephones, etc. are usually available to communicate notifications. Option C is a manageable problem that requires additional funding, but can be addressed. Option D is a problem that can be addressed. Most hosting providers have standardized the level of physical security that is in place. Regular physical audits or a SAS 70 report can address such concerns.

QUESTION 33
Effective IT governance is BEST ensured by:

A. utilizing a bottom-up approach.

B. management by the IT department.
C. referring the matter to the organization's legal department.
D. utilizing a top-down approach.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Effective IT governance needs to be a top-down initiative, with the board and executive management setting clear policies, goals and objectives and providing for ongoing monitoring of the same. Focus on the regulatory issues and management priorities may not be reflected effectively by a bottom-up approach. IT governance affects the entire organization and is not a matter concerning only the management of IT. The legal department is part of the overall governance process, but cannot take full responsibility.

QUESTION 34
The FIRST step to create an internal culture that focuses on information security is to:

A. implement stronger controls.
B. conduct periodic awareness training.
C. actively monitor operations.
D. gain the endorsement of executive management.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

QUESTION 35
Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

A. Obtain the support of the board of directors.
B. Improve the content of the information security awareness program.

C. Improve the employees' knowledge of security policies.
D. Implement logical access controls to the information systems.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

It is extremely difficult to implement an information security program without the aid and support of the board of directors. If they do not understand the importance of security to the achievement of the business objectives, other measures will not be sufficient. Options B and (' are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

QUESTION 36
When an organization is implementing an information security governance program, its board of directors should be responsible for:

A. drafting information security policies.
B. reviewing training and awareness programs.
C. setting the strategic direction of the program.
D. auditing for compliance.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A board of directors should establish the strategic direction of the program to ensure that it is in sync with the company's vision and business goals. The board must incorporate the governance program into the overall corporate business strategy. Drafting information security policies is best fulfilled by someone such as a security manager with the expertise to bring balance, scope and focus to the policies. Reviewing training and awareness programs may best be handled by security management and training staff to ensure that the training is on point and follows best practices. Auditing for compliance is best left to the internal and external auditors to provide an objective review of the program and how it meets regulatory and statutory compliance.

QUESTION 37

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BEST approach of the information security manager?

A. Acceptance of the business manager's decision on the risk to the corporation
B. Acceptance of the information security manager's decision on the risk to the corporation
C. Review of the assessment with executive management for final input
D. A new risk assessment and BIA are needed to resolve the disagreement

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

QUESTION 38
Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

A. The security officer
B. Senior management
C. The end user
D. The custodian

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Routine administration of all aspects of security is delegated, but top management must retain overall responsibility. The security officer supports and implements information security for senior management. The end user does not perform categorization. The custodian supports and implements information security measures as directed.

QUESTION 39
An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

A. Direct information security on what they need to do
B. Research solutions to determine the proper solutions
C. Require management to report on compliance
D. Nothing; information security does not report to the board

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Information security governance is the responsibility of the board of directors and executive management. In this instance, the appropriate action is to ensure that a plan is in place for implementation of needed safeguards and to require updates on that implementation.

QUESTION 40
Information security should be:

A. focused on eliminating all risks.
B. a balance between technical and business requirements.
C. driven by regulatory requirements.
D. defined by the board of directors.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Information security should ensure that business objectives are met given available technical capabilities, resource constraints and compliance requirements. It is not practical or feasible to eliminate all risks. Regulatory requirements must be considered, but are inputs to the business considerations. The board of directors does not define information security, but provides direction in support of the business goals and objectives.

QUESTION 41
What is the MOST important factor in the successful implementation of an enterprise wide information security program?

A. Realistic budget estimates
B. Security awareness
C. Support of senior management
D. Recalculation of the work factor

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Without the support of senior management, an information security program has little chance of survival. A company's leadership group, more than any other group, will more successfully drive the program. Their authoritative position in the company is a key factor. Budget approval, resource commitments, and companywide participation also require the buy-in from senior management. Senior management is responsible for providing an adequate budget and the necessary resources. Security awareness is important, but not the most important factor. Recalculation of the work factor is a part of risk management.

QUESTION 42
What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

A. Functional requirements are not adequately considered.
B. User training programs may be inadequate.
C. Budgets allocated to business units are not appropriate.
D. Information security plans are not aligned with business requirements

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The steering committee controls the execution of the information security strategy, according to the needs of the organization, and decides on the project prioritization and the execution plan. User management is an important group that should be represented to ensure that the information security plans are aligned

with the business needs. Functional requirements and user training programs are considered to be part of the projects but are not the main risks. The steering committee does not approve budgets for business units.

QUESTION 43
The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

A. the plan aligns with the organization's business plan.
B. departmental budgets are allocated appropriately to pay for the plan.
C. regulatory oversight requirements are met.
D. the impact of the plan on the business units is reduced.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The steering committee controls the execution of the information security strategy according to the needs of the organization and decides on the project prioritization and the execution plan. The steering committee does not allocate department budgets for business units. While ensuring that regulatory oversight requirements are met could be a consideration, it is not the main reason for the review. Reducing the impact on the business units is a secondary concern but not the main reason for the review.

QUESTION 44
Which of the following should be determined while defining risk management strategies?

A. Risk assessment criteria
B. Organizational objectives and risk appetite
C. IT architecture complexity
D. Enterprise disaster recovery plans

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

While defining risk management strategies, one needs to analyze the organization's objectives and risk appetite and define a risk management framework based on this analysis. Some organizations may accept known risks, while others may invest in and apply mitigation controls to reduce risks. Risk assessment criteria would become part of this framework, but only after proper analysis. IT architecture complexity and enterprise disaster recovery plans are more directly related to assessing risks than defining strategies.

QUESTION 45
When implementing effective security governance within the requirements of the company's security strategy, which of the following is the MOST important factor to consider?

A. Preserving the confidentiality of sensitive data
B. Establishing international security standards for data sharing
C. Adhering to corporate privacy standards
D. Establishing system manager responsibility for information security

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The goal of information security is to protect the organization's information assets. International security standards are situational, depending upon the company and its business. Adhering to corporate privacy standards is important, but those standards must be appropriate and adequate and are not the most important factor to consider. All employees are responsible for information security, but it is not the most important factor to consider.

QUESTION 46
Which of the following is the BEST reason to perform a business impact analysis (BIA)?

A. To help determine the current state of risk
B. To budget appropriately for needed controls
C. To satisfy regulatory requirements
D. To analyze the effect on the business

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The BIA is included as part of the process to determine the current state of risk and helps determine the acceptable levels of response from impacts and the current level of response, leading to a gap analysis. Budgeting appropriately may come as a result, but is not the reason to perform the analysis. Performing an analysis may satisfy regulatory requirements, bill is not the reason to perform one. Analyzing the effect on the business is part of the process, but one must also determine the needs or acceptable effect or response.

QUESTION 47
Which of the following **BEST** enables the deployment of consistent security throughout international branches within a multinational organization?

A. Maturity of security processes
B. Remediation of audit findings
C. Decentralization of security governance
D. Establishment of security governance

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is the BEST way to determine if an information security program aligns with corporate governance?

A. Evaluate funding for security initiatives
B. Survey end users about corporate governance
C. Review information security policies
D. Review the balanced scorecard

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation

One of the most important aspects of the action plan to execute the strategy is to create or modify, as needed, policies and standards. Policies are one of the primary elements of governance and each policy should state only one general security mandate. The road map should show the steps and the sequence, dependencies, and milestones.

QUESTION 49
Security governance is MOST associated with which of the following IT infrastructure components?

A. Network
B. Application
C. Platform
D. Process

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

A. An emerging technologies strategy is in place
B. An effective security risk management process is established
C. End user acceptance of emerging technologies is established
D. A cost-benefit analysis process is easier to perform

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 51
The MOST important element in achieving executive commitment to an information security governance program is:

A. identified business drivers
B. a process improvement model
C. established security strategies
D. a defined security framework

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 52
Which of the following is the MOST appropriate board-level activity for information security governance?

A. Establish security and continuity ownership
B. Develop “what-if” scenarios on incidents
C. Establish measures for security baselines
D. Include security in job-performance appraisals

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 53

Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

A. Implementing additional security awareness training
B. Communicating critical risk assessment results to business unit managers
C. Including business unit representation on the security steering committee
D. Publishing updated information security policies

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:

QUESTION 54
In addition to business alignment and security ownership, which of the following is MOST critical for information security governance?

A. Auditability of systems
B. Compliance with policies
C. Reporting of security metrics
D. Executive sponsorship

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 55
Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

A. Areas of highest risk may not be adequately prioritized for treatment
B. Redundant controls may be implemented across divisions
C. Information security governance could be decentralized by division
D. Return on investment may be inconsistently reported to senior management

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 56
The effectiveness of an information security governance framework will BEST be enhanced if:

A. IS auditors are empowered to evaluate governance activities
B. risk management is built into operational and strategic activities
C. a culture of legal and regulatory compliance is promoted by management
D. consultants review the information security governance framework

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 57
When developing an information security governance framework, which of the following would be the **MAIN** impact when lacking senior management involvement?

A. Accountability for risk treatment is not clearly defined.
B. Information security responsibilities are not communicated effectively.
C. Resource requirements are not adequately considered.
D. Information security plans do not support business requirements.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 58

Which of the following is the **BEST** way to facilitate the alignment between an organization's information security program and business objectives?

A. Information security is considered at the feasibility stage of all IT projects.
B. The information security governance committee includes representation from key business areas.
C. The chief executive officer reviews and approves the information security program.
D. The information security program is audited by the internal audit department.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
QUESTION 59
The effectiveness of the information security process is reduced when an outsourcing organization:

A. is responsible for information security governance activities
B. receives additional revenue when security service levels are met
C. incurs penalties for failure to meet security service-level agreements
D. standardizes on a single access-control software product

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 60
What should be an information security manager's FIRST course of action when an organization is subject to a new regulatory requirement?

A. Perform a gap analysis
B. Complete a control assessment
C. Submit a business case to support compliance
D. Update the risk register

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 61
Internal audit has reported a number of information security issues which are not in compliance with regulatory requirements. What should the information security manager do FIRST?

A. Create a security exception
B. Perform a vulnerability assessment
C. Perform a gap analysis to determine needed resources
D. Assess the risk to business operations

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 62
A risk mitigation report would include recommendations for:

A. assessment.
B. acceptance.
C. evaluation.
D. quantification.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment. evaluation and risk quantification are components of the risk analysis process that are completed prior to determining risk mitigation solutions.

QUESTION 63
A risk management program should reduce risk to:

A. zero.
B. an acceptable level.
C. an acceptable percent of revenue.
D. an acceptable probability of occurrence.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk should be reduced to an acceptable level based on the risk preference of the organization. Reducing risk to zero is impractical and could be cost-prohibitive. Tying risk to a percentage of revenue is inadvisable since there is no direct correlation between the two. Reducing the probability of risk occurrence may not always be possible, as in the ease of natural disasters. The focus should be on reducing the impact to an acceptable level to the organization, not reducing the probability of the risk.

QUESTION 64
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precise.
B. security risks are subject to frequent change.
C. reviewers can optimize and reduce the cost of controls.
D. it demonstrates to senior management that the security function can add value.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

QUESTION 65
Which of the following BEST indicates a successful risk management practice?

A. Overall risk is quantified
B. Inherent risk is eliminated
C. Residual risk is minimized
D. Control risk is tied to business units

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A successful risk management practice minimizes the residual risk to the organization. Choice A is incorrect because the fact that overall risk has been quantified does not necessarily indicate the existence of a successful risk management practice. Choice B is incorrect since it is virtually impossible to eliminate inherent risk. Choice D is incorrect because, although the tying of control risks to business may improve accountability, this is not as desirable as minimizing residual risk.

QUESTION 66
Which of the following would generally have the GREATEST negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services
C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Although the theft of software, interruption of utility services and internal frauds are all significant, the loss of customer confidence is the most damaging and could cause the business to fail.

QUESTION 67

A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results
D. Amount of IT budget available

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

QUESTION 68
Which of the following will BEST protect an organization from internal security attacks?

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employee awareness certification program

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Because past performance is a strong predictor of future performance, background checks of prospective employees best prevents attacks from originating within an organization. Static IP addressing does little to prevent an internal attack. Internal address translation using non-routable addresses is useful against external attacks but not against internal attacks. Employees who certify that they have read security policies are desirable, but this does not guarantee that the employees behave honestly.

QUESTION 69
For risk management purposes, the value of an asset should be based on:

A. original cost.
B. net cash flow.
C. net present value.D. replacement cost.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

QUESTION 70
In a business impact analysis, the value of an information system should be based on the overall cost:

A. of recovery.
B. to recreate.
C. if unavailable.
D. of emergency operations.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The value of an information system should be based on the cost incurred if the system were to become unavailable. The cost to design or recreate the system is not as relevant since a business impact analysis measures the impact that would occur if an information system were to become unavailable. Similarly, the cost of emergency operations is not as relevant.

QUESTION 71
Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.
C. control risk is minimized.
D. inherent risk is minimized.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Residual risk is the risk that remains after putting into place an effective risk management program; therefore, acceptable risk is achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party and may not necessarily be equal to the minimal form of residual risk. Control risk is the risk that controls may not prevent/detect an incident with a measure of control effectiveness. Inherent risk cannot be minimized.

QUESTION 72
The value of information assets is BEST determined by:

A. individual business managers.
B. business systems analysts.
C. information security management.
D. industry averages benchmarking.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Individual business managers are in the best position to determine the value of information assets since they are most knowledgeable of the assets' impact on the business. Business systems developers and information security managers are not as knowledgeable regarding the impact on the business. Peer companies' industry averages do not necessarily provide detailed enough information nor are they as relevant to the unique aspects of the business.

QUESTION 73
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

A. Feasibility
B. Design
C. Development
D. Testing

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

QUESTION 74
The MOST effective way to incorporate risk management practices into existing production systems is through:

A. policy development.
B. change management.
C. awareness training.
D. regular monitoring.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

QUESTION 75
Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

A. Gap analysis
B. Regression analysis
C. Risk analysis
D. Business impact analysis

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Recovery time objectives (RTOs) are a primary deliverable of a business impact analysis. RTOs relate to the financial impact of a system not being available. A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules. Risk analysis is a component of the business impact analysis.

QUESTION 76
The recovery time objective (RTO) is reached at which of the following milestones?

A. Disaster declaration
B. Recovery of the backups
C. Restoration of the system
D. Return to business as usual processing

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The recovery time objective (RTO) is based on the amount of time required to restore a system; disaster declaration occurs at the beginning of this period. Recovery of the backups occurs shortly after the beginning of this period. Return to business as usual processing occurs significantly later than the RTO. RTO is an "objective," and full restoration may or may not coincide with the RTO. RTO can be the minimum acceptable operational level, far short of normal operations.

QUESTION 77
Which of the following results from the risk assessment process would BEST assist risk management decision making?

A. Control risk
B. Inherent risk
C. Risk exposure
D. Residual risk

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

QUESTION 78
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

A. Business continuity coordinator
B. Chief operations officer (COO)
C. Information security manager
D. Internal audit

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The recovery point objective (RPO) is the processing checkpoint to which systems are recovered. In addition to data owners, the chief operations officer (COO) is the most knowledgeable person to make this decision. It would be inappropriate for the information security manager or an internal audit to determine the RPO because they are not directly responsible for the data or the operation.

QUESTION 79
Which two components PRIMARILY must be assessed in an effective risk analysis?

A. Visibility and duration
B. Likelihood and impact
C. Probability and frequency
D. Financial impact and duration

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The probability or likelihood of the event and the financial impact or magnitude of the event must be assessed first. Duration refers to the length of the event; it is important in order to assess impact but is secondary. Once the likelihood is determined, the frequency is also important to determine overall impact.

QUESTION 80
Information security managers should use risk assessment techniques to:
A. justify selection of risk mitigation strategies.
B. maximize the return on investment (ROD.
C. provide documentation for auditors and regulators.
D. quantify risks that would otherwise be subjective.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

QUESTION 81
In assessing risk, it is MOST essential to:

A. provide equal coverage for all asset types.
B. use benchmarking data from similar organizations.
C. consider both monetary value and likelihood of loss.
D. focus primarily on threats and recent business losses.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A risk analysis should take into account the potential financial impact and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus primarily on recent losses or losses experienced by similar firms. Although this is important supplementary information, it does not reflect the organization's real situation. Geography and other factors come into play as well.

QUESTION 82
When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

A. the information security steering committee.
B. customers who may be impacted.
C. data owners who may be impacted.
D. regulatory- agencies overseeing privacy.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

QUESTION 83
Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Data owners are responsible for assigning user entitlements and approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

QUESTION 84
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

A. IT assets in key business functions are protected.
B. business risks are addressed by preventive controls.
C. stated objectives are achievable.
D. IT facilities and systems are always available.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk management's primary goal is to ensure an organization maintains the ability to achieve its objectives. Protecting IT assets is one possible goal as well as ensuring infrastructure and systems availability. However, these should be put in the perspective of achieving an organization's objectives. Preventive controls are not always possible or necessary; risk management will address issues with an appropriate mix of preventive and corrective controls.

QUESTION 85
It is important to classify and determine relative sensitivity of assets to ensure that:

A. cost of protection is in proportion to sensitivity.
B. highly sensitive assets are protected.
C. cost of controls is minimized.
D. countermeasures are proportional to risk.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

QUESTION 86
The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

A. ensure the provider is made liable for losses.
B. recommend not renewing the contract upon expiration.
C. recommend the immediate termination of the contract.
D. determine the current level of security.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

QUESTION 87
An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

A. threat.
B. loss.
C. vulnerability.
D. probability.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Implementing more restrictive preventive controls mitigates vulnerabilities but not the threats. Losses and probability of occurrence may not be primarily or directly affected.

QUESTION 88
When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

A. Evaluate productivity losses
B. Assess the impact of confidential data disclosure
C. Calculate the value of the information or asset
D. Measure the probability of occurrence of each threat

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Calculating the value of the information or asset is the first step in a risk analysis process to determine the impact to the organization, which is the ultimate goal. Determining how much productivity could be lost and how much it would cost is a step in the estimation of potential risk process. Knowing the impact if confidential information is disclosed is also a step in the estimation of potential risk. Measuring the probability of occurrence for each threat identified is a step in performing a threat analysis and therefore a partial answer.

QUESTION 89
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

A. map the major threats to business objectives.
B. review available sources of risk information.
C. identify the value of the critical assets.
D. determine the financial impact if threats materialize.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

QUESTION 90
The valuation of IT assets should be performed by:

A. an IT security manager.
B. an independent security consultant.
C. the chief financial officer (CFO).
D. the information owner.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

QUESTION 91
The PRIMARY objective of a risk management program is to:

A. minimize inherent risk.
B. eliminate business risk.
C. implement effective controls.
D. minimize residual risk.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The goal of a risk management program is to ensure that residual risk remains within manageable levels. Management of risk does not always require the removal of inherent risk nor is this always possible. A possible benefit of good risk management is to reduce insurance premiums, but this is not its primary intention. Effective controls are naturally a clear objective of a risk management program, but with the choices given, choice C is an incomplete answer.

QUESTION 92
After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

A. Senior management
B. Business manager
C. IT audit manager
D. Information security officer (ISO)

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The business manager will be in the best position, based on the risk assessment and mitigation proposals. to decide which controls should/could be implemented, in line with the business strategy and with budget. Senior management will have to ensure that the business manager has a clear understanding of the risk assessed but in no case will be in a position to decide on specific controls. The IT audit manager will take part in the process to identify threats and vulnerabilities, and to make recommendations for mitigations. The information security officer (ISO) could make some decisions regarding implementation of controls. However, the business manager will have a broader business view and full control over the budget and, therefore, will be in a better position to make strategic decisions.

QUESTION 93
When performing an information risk analysis, an information security manager should FIRST:

A. establish the ownership of assets.
B. evaluate the risks to the assets.
C. take an asset inventory.
D. categorize the assets.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Assets must be inventoried before any of the other choices can be performed.

QUESTION 94
The PRIMARY benefit of performing an information asset classification is to:

A. link security requirements to business objectives.
B. identify controls commensurate to risk.
C. define access rights.
D. establish ownership.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

All choices are benefits of information classification. However, identifying controls that are proportional to the risk in all cases is the primary benefit of the process.

QUESTION 95
Which of the following is MOST essential for a risk management program to be effective?

A. Flexible security budget
B. Sound risk baseline
C. New risks detection
D. Accurate risk reporting

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

All of these procedures are essential for implementing risk management. However, without identifying new risks, other procedures will only be useful for a limited period.

QUESTION 96
Which of the following attacks is BEST mitigated by utilizing strong passwords?

A. Man-in-the-middle attack
B. Brute force attack
C. Remote buffer overflow
D. Root kit

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A brute force attack is normally successful against weak passwords, whereas strong passwords would not prevent any of the other attacks. Man-in-the-middle attacks intercept network traffic, which could contain passwords, but is not naturally password-protected. Remote buffer overflows rarely require a password to exploit a remote host. Root kits hook into the operating system's kernel and, therefore, operate underneath any authentication mechanism.

QUESTION 97
Phishing is BEST mitigated by which of the following?

A. Security monitoring software
B. Encryption
C. Two-factor authentication
D. User awareness

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.

QUESTION 98
The security responsibility of data custodians in an organization will include:

A. assuming overall protection of information assets.
B. determining data classification levels.
C. implementing security controls in products they install. D. ensuring security measures are consistent with policy.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security responsibilities of data custodians within an organization include ensuring that appropriate security measures are maintained and are consistent with organizational policy. Executive management holds overall responsibility for protection of the information assets. Data owners determine data classification levels

for information assets so that appropriate levels of controls can be provided to meet the requirements relating to confidentiality, integrity and availability. Implementation of information security in products is the responsibility of the IT developers.

QUESTION 99

A security risk assessment exercise should be repeated at regular intervals because:

A. business threats are constantly changing.
B. omissions in earlier assessments can be addressed.
C. repetitive assessments allow various methodologies.
D. they help raise awareness on security in the business.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

As business objectives and methods change, the nature and relevance of threats change as well. Choice B does not, by itself, justify regular reassessment. Choice C is not necessarily true in all cases. Choice D is incorrect because there are better ways of raising security awareness than by performing a risk assessment.

QUESTION 100

Which of the following steps in conducting a risk assessment should be performed FIRST?

A. Identity business assets
B. Identify business risks
C. Assess vulnerabilities
D. Evaluate key controls

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

QUESTION 101
The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:
A. periodically testing the incident response plans.
B. regularly testing the intrusion detection system (IDS).
C. establishing mandatory training of all personnel.
D. periodically reviewing incident response procedures.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security incident response plans should be tested to find any deficiencies and improve existing processes. Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation. All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended. Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

QUESTION 102
Which of the following risks is represented in the risk appetite of an organization?

A. Control
B. Inherent
C. Residual
D. Audit

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Residual risk is unmanaged, i.e., inherent risk which remains uncontrolled. This is key to the organization's risk appetite and is the amount of residual risk that a business is living with that affects its viability. Hence, inherent risk is incorrect. Control risk, the potential for controls to fail, and audit risk, which relates only to audit's approach to their work, are not relevant in this context.

QUESTION 103
Which of the following would a security manager establish to determine the target for restoration of normal processing?
A. Recover time objective (RTO)
B. Maximum tolerable outage (MTO)
C. Recovery point objectives (RPOs)
D. Services delivery objectives (SDOs)

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

QUESTION 104
A risk management program would be expected to:

A. remove all inherent risk.
B. maintain residual risk at an acceptable level.
C. implement preventive controls for every threat.
D. reduce control risk to zero.

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

QUESTION 105
Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

A. Programming
B. Specification
C. User testing
D. Feasibility

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk should be addressed as early as possible in the development cycle. The feasibility study should include risk assessment so that the cost of controls can be estimated before the project proceeds. Risk should also be considered in the specification phase where the controls are designed, but this would still be based on the assessment carried out in the feasibility study. Assessment would not be relevant in choice A or C.

QUESTION 106
Which of the following would help management determine the resources needed to mitigate a risk to the organization?

A. Risk analysis process
B. Business impact analysis (BIA)
C. Risk management balanced scorecard
D. Risk-based audit program

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

QUESTION 107
A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

A. there are sufficient safeguards in place to prevent this risk from happening.
B. the needed countermeasure is too complicated to deploy.
C. the cost of countermeasure outweighs the value of the asset and potential loss.
D. The likelihood of the risk occurring is unknown.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

QUESTION 108
Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

A. Number of controls implemented
B. Percent of control objectives accomplished
C. Percent of compliance with the security policy
D. Reduction in the number of reported security incidents

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

QUESTION 109
Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

A. Strategic business plan
B. Upcoming financial results
C. Customer personal information
D. Previous financial results

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Previous financial results are public; all of the other choices are private information and should only be accessed by authorized entities.

QUESTION 110
The PRIMARY purpose of using risk analysis within a security program is to:

A. justify the security expenditure.
B. help businesses prioritize the assets to be protected.
C. inform executive management of residual risk value.
D. assess exposures and plan remediation.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

QUESTION 111
Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?
A. Defining job roles
B. Performing a risk assessment
C. Identifying data owners
D. Establishing data retention policies

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Identifying the data owners is the first step, and is essential to implementing data classification. Defining job roles is not relevant. Performing a risk assessment is important, but will require the participation of data owners (who must first be identified). Establishing data retention policies may occur after data have been classified.

QUESTION 112
An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

A. mitigate the impact by purchasing insurance.
B. implement a circuit-level firewall to protect the network.
C. increase the resiliency of security measures in place.
D. implement a real-time intrusion detection system.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Since residual risk will always be too high, the only practical solution is to mitigate the financial impact by purchasing insurance.

QUESTION 113
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

A. Business impact analyses

B. Security gap analyses
C. System performance metrics
D. Incident response processes

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A security gap analysis is a process which measures all security controls in place against typically good business practice, and identifies related weaknesses. A business impact analysis is less suited to identify security deficiencies. System performance metrics may indicate security weaknesses, but that is not their primary purpose. Incident response processes exist for cases where security weaknesses are exploited.

QUESTION 114
A common concern with poorly written web applications is that they can allow an attacker to:

A. gain control through a buffer overflow.
B. conduct a distributed denial of service (DoS) attack.
C. abuse a race condition.
D. inject structured query language (SQL) statements.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Structured query language (SQL) injection is one of the most common and dangerous web application vulnerabilities. Buffer overflows and race conditions are very difficult to find and exploit on web applications. Distributed denial of service (DoS) attacks have nothing to do with the quality of a web application.

QUESTION 115
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

A. Historical cost of the asset
B. Acceptable level of potential business impacts
C. Cost versus benefit of additional mitigating controls

D.
Annualized loss expectancy (ALE)

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

QUESTION 116
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

A. Understand the business requirements of the developer portal
B. Perform a vulnerability assessment of the developer portal
C. Install an intrusion detection system (IDS)
D. Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

QUESTION 117
A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

A. Prevent the system from being accessed remotely

D.
B. Create a strong random password
C. Ask for a vendor patch
Track usage of the account by audit trails

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

QUESTION 118
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

A. a lack of proper input validation controls.
B. weak authentication controls in the web application layer.
C. flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.
D. implicit web application trust relationships.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

QUESTION 119

D.

Which of the following would BEST address the risk of data leakage?

A. File backup procedures
B. Database integrity checks
C. Acceptable use policies
Incident response procedures

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

QUESTION 120
A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

A. Access control policy
B. Data classification policy
C. Encryption standards
D. Acceptable use policy

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Data classification policies define the level of protection to be provided for each category of data. Without this mandated ranking of degree of protection, it is difficult to determine what access controls or levels of encryption should be in place. An acceptable use policy is oriented more toward the end user and, therefore, would not specifically address what controls should be in place to adequately protect information.

D.

QUESTION 121

What is the BEST technique to determine which security controls to implement with a limited budget?

A. Risk analysis
B. Annualized loss expectancy (ALE) calculations
C. Cost-benefit analysis
D. Impact analysis

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

QUESTION 122
A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

A. A penetration test
B. A security baseline review
C. A risk assessment
D. A business impact analysis (BIA)

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A risk assessment will identify- the business impact of such vulnerability being exploited and is, thus, the correct process. A penetration test or a security baseline review may identify the vulnerability but not the remedy. A business impact analysis (BIA) will more likely identify the impact of the loss of the mail server.

QUESTION 123
Which of the following measures would be MOST effective against insider threats to confidential information?

A. Role-based access control
B. Audit trail monitoring
C. Privacy policy
D. Defense-in-depth**Correct Answer:** A **Section: INFORMATION RISK MANAGEMENT Explanation**

Explanation/Reference:
Explanation:

Role-based access control provides access according to business needs; therefore, it reduces unnecessary- access rights and enforces accountability. Audit trail monitoring is a detective control, which is 'after the fact.' Privacy policy is not relevant to this risk. Defense-in-depth primarily focuses on external threats

QUESTION 124
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

A. conduct a risk assessment and allow or disallow based on the outcome.
B. recommend a risk assessment and implementation only if the residual risks are accepted.
C. recommend against implementation because it violates the company's policies.
D. recommend revision of current policy.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

QUESTION 125
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

A. increase its customer awareness efforts in those regions.
B. implement monitoring techniques to detect and react to potential fraud.
C. outsource credit card processing to a third party.
D. make the customer liable for losses if they fail to follow the bank's advice.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk. Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

QUESTION 126
The criticality and sensitivity of information assets is determined on the basis of:

A. threat assessment.
B. vulnerability assessment.
C. resource dependency assessment.
D. impact assessment.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

QUESTION 127
Which program element should be implemented FIRST in asset classification and control?

A. Risk assessment
B. Classification
C. Valuation
D. Risk mitigation

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT

Explanation

Explanation/Reference:
Explanation:

Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

QUESTION 128
When performing a risk assessment, the MOST important consideration is that:

A. management supports risk mitigation efforts.
B. annual loss expectations (ALEs) have been calculated for critical assets.
C. assets have been identified and appropriately valued.
D. attack motives, means and opportunities be understood.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. ALE calculations are only valid if assets have first been identified and appropriately valued. Motives, means and opportunities should already be factored in as a part of a risk assessment.

QUESTION 129
The MAIN reason why asset classification is important to a successful information security program is because classification determines:

A. the priority and extent of risk mitigation efforts.
B. the amount of insurance needed in case of loss.
C. the appropriate level of protection to the asset.
D. how protection levels compare to peer organizations.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Protection should be proportional to the value of the asset. Classification is based upon the value of the asset to the organization. The amount of insurance needed in case of loss may not be applicable in each case. Peer organizations may have different classification schemes for their assets.

QUESTION 130
The BEST strategy for risk management is to:

A. achieve a balance between risk and organizational goals.
B. reduce risk to an acceptable level.
C. ensure that policy development properly considers organizational risks.
D. ensure that all unmitigated risks are accepted by management.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to l>e considered a strategy.

QUESTION 131
Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

A. Disclosure of personal information
B. Sufficient coverage of the insurance policy for accidental losses
C. Intrinsic value of the data stored on the equipment
D. Replacement cost of the equipment

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
When mobile equipment is lost or stolen, the information contained on the equipment matters most in determining the impact of the loss. The more sensitive the information, the greater the liability. If staff carries mobile equipment for business purposes, an organization must develop a clear policy as to what information should be kept on the equipment and for what purpose. Personal information is not defined in the question as the data that were lost. Insurance may be a relatively smaller issue as compared with information theft or opportunity loss, although insurance is also an important factor for a successful business. Cost of equipment would be a less important issue as compared with other choices.

QUESTION 132
An organization has to comply with recently published industry regulatory requirements — compliance that potentially has high implementation costs. What should the information security manager do FIRST?

A. Implement a security committee.
B. Perform a gap analysis.
C. Implement compensating controls.
D. Demand immediate compliance.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Since they are regulatory requirements, a gap analysis would be the first step to determine the level of compliance already in place. Implementing a security committee or compensating controls would not be the first step. Demanding immediate compliance would not assess the situation.

QUESTION 133
Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

A. Annual loss expectancy (ALE) of incidents
B. Frequency of incidents
C. Total cost of ownership (TCO)
D. Approved budget for the project

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
The total cost of ownership (TCO) would be the most relevant piece of information in that it would establish a cost baseline and it must be considered for the full life cycle of the control. Annual loss expectancy (ALE) and the frequency of incidents could help measure the benefit, but would have more of an indirect relationship as not all incidents may be mitigated by implementing a two-factor authentication system. The approved budget for the project may have no bearing on what the project may actually cost.

QUESTION 134
Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

A. Senior management support
B. Results of a cost-benefit analysis
C. Results of a risk assessment
D. Impact on the risk profile

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation
The information security manager must understand the business risk profile of the organization. No model provides a complete picture, but logically categorizing the risk areas of an organization facilitates focusing on key risk management strategies and decisions. It also enables the organization to develop and implement risk treatment approaches that are relevant to the business and cost effective.

QUESTION 135
It is MOST important for an information security manager to ensure that security risk assessments are performed:

A. consistently throughout the enterprise
B. during a root cause analysis
C. as part of the security business case
D. in response to the threat landscape

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

Reference *https://m.isaca.org/Certification/Additional-Resources/Documents/CISM-Item-Development-Guide_bro_Eng_0117.pdf* (14)

QUESTION 136
An information security manager has been asked to create a strategy to protect the organization's information from a variety of threat vectors. Which of the following should be done FIRST?

A. Perform a threat modeling exercise
B. Develop a risk profile
C. Design risk management processes
D. Select a governance framework

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 137
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

A. Integrating the risk assessment into the internal audit program
B. Applying global security standards to the IT projects
C. Training project managers on risk assessment
D. Having the information security manager participate on the project setting committees

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 138
An information security manager has completed a risk assessment and has determined the residual risk. Which of the following should be the NEXT step?

A. Conduct an evaluation of controls
B. Determine if the risk is within the risk appetite
C. Implement countermeasures to mitigate risk
D. Classify all identified risks

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 139
Which of the following would be the BEST indicator that an organization is appropriately managing risk?

A. The number of security incident events reported by staff has increased
B. Risk assessment results are within tolerance
C. A penetration test does not identify any high-risk system vulnerabilities
D. The number of events reported from the intrusion detection system has declined

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 140
A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

A. higher costs in supporting end users
B. impact on network capacity
C. decrease in end user productivity
D. lack of a device management solution

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:
Reference https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

QUESTION 141
Which of the following vulnerabilities presents the GREATEST risk of external hackers gaining access to the corporate network?

A. Internal hosts running unnecessary services
B. Inadequate logging
C. Excessive administrative rights to an internal database
D. Missing patches on a workstation

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 142
An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be MOST important to include when presenting the strategy to senior management?

A. The costs associated with business process changes
B. Results of benchmarking against industry peers
C. The impact of organizational changes on the security risk profile
D. Security controls needed for risk mitigation

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 143
What is the BEST way to determine the level of risk associated with information assets processed by an IT application?

A. Evaluate the potential value of information for an attacker
B. Calculate the business value of the information assets
C. Review the cost of acquiring the information assets for the business
D. Research compliance requirements associated with the information

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 144
When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

A. monitor for business changes
B. review the residual risk level
C. report compliance to management
D. implement controls to mitigate the risk

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 145
Which of the following would be MOST useful in a report to senior management for evaluating changes in the organization's information security risk position?

A. Risk register
B. Trend analysis
C. Industry benchmarks
D. Management action plan

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 146
An information security manager is preparing a presentation to obtain support for a security initiative. Which of the following would be the BEST way to obtain management's commitment for the initiative?

A. Include historical data of reported incidents
B. Provide the estimated return on investment
C. Provide an analysis of current risk exposures
D. Include industry benchmarking comparisons

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 147
Which of the following is the MOST significant security risk in IT asset management?

A. IT assets may be used by staff for private purposes
B. Unregistered IT assets may not be supported
C. Unregistered IT assets may not be included in security documentation
D. Unregistered IT assets may not be configured properly

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 148
Which of the following is the MOST effective method of preventing deliberate internal security breaches?

A. Screening prospective employees
B. Well-designed firewall system
C. Well-designed intrusion detection system (IDS)
D. Biometric security access control

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Reference https://www.techrepublic.com/article/strategies-for-preventing-internal-security-breaches-in-a-growing-business/

QUESTION 149
A business previously accepted the risk associated with a zero-day vulnerability. The same vulnerability was recently exploited in a high-profile attack on another organization in the same industry. Which of the following should be the information security manager's FIRST course of action?

A. Reassess the risk in terms of likelihood and impact
B. Develop best and worst case scenarios
C. Report the breach of the other organization to senior management
D. Evaluate the cost of remediating the vulnerability

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 150
To effectively manage an organization's information security risk, it is MOST important to:

A. periodically identify and correct new systems vulnerabilities
B. assign risk management responsibility to end users

C. benchmark risk scenarios against peer organizations
D. establish and communicate risk tolerance

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 151
Which of the following is the BEST course of action for the information security manager when residual risk is above the acceptable level of risk?

A. Perform cost-benefit analysis
B. Recommend additional controls
C. Carry out risk assessment
D. Defer to business management

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 152
Which of the following is the BEST reason to initiate a reassessment of current risk?

A. Follow-up to an audit report
B. A recent security incident
C. Certification requirements
D. Changes to security personnel

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 153
Before final acceptance of residual risk, what is the **BEST** way for an information security manager to address risk factors determined to be lower than acceptable risk levels?

A. Evaluate whether an excessive level of control is being applied.
B. Ask senior management to increase the acceptable risk levels.
C. Implement more stringent countermeasures.
D. Ask senior management to lower the acceptable risk levels.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 154
When selecting risk response options to manage risk, an information security manager's **MAIN** focus should be on reducing:

A. exposure to meet risk tolerance levels.
B. the likelihood of threat.
C. financial loss by transferring risk.
D. the number of security vulnerabilities.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 155
Which of the following should an information security manager perform **FIRST** when an organization's residual risk has increased?

A. Implement security measures to reduce the risk.
B. Communicate the information to senior management.
C. Transfer the risk to third parties.
D. Assess the business impact.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 156
Which of the following approaches is **BEST** for selecting controls to minimize information security risks?

A. Cost-benefit analysis
B. Control-effectiveness
C. Risk assessment
D. Industry best practices

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 157
Which of the following is the **MOST** appropriate course of action when the risk occurrence rate is low but the impact is high?

A. Risk transfer
B. Risk acceptance
C. Risk mitigation
D. Risk avoidance

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 158

Which of the following is the **MOST** effective way to communicate information security risk to senior management?

A. Business impact analysis
B. Balanced scorecard
C. Key performance indicators (KPIs)
D. Heat map

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 159
Security risk assessments should cover only information assets that:

A. are classified and labeled.
B. are inside the organization.
C. support business processes.
D. have tangible value.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 160
Which of the following is an indicator of improvement in the ability to identify security risks?

A. Increased number of reported security incidents.
B. Decreased number of staff requiring information security training.
C. Decreased number of information security risk assessments.
D. Increased number of security audit issues resolved.

Correct Answer: D

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 161

Which of the following is the **MOST** important step in risk ranking?

A. Impact assessment
B. Mitigation cost
C. Threat assessment
D. Vulnerability analysis

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 162

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the **BEST** information to help maintain the security posture?

A. Risk assessment
B. Cloud security strategy
C. Vulnerability assessment
D. Risk governance framework

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 163

Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:

A. inform senior management
B. update the risk assessment
C. validate the user acceptance testing
D. modify key risk indicators

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 164
Which of the following would BEST mitigate identified vulnerabilities in a timely manner?

A. Continuous vulnerability monitoring tool
B. Categorization of the vulnerabilities based on system's criticality
C. Monitoring of key risk indicators (KRIs)
D. Action plan with responsibilities and deadlines

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanations
One approach seeing increasing use is to report and monitor risk through the use of key risk indicators (KRIs). KRIs can be defined as measures that, in some manner, indicate when an enterprise is subject to risk that exceeds a defined risk level. Typically, these indicators are trends in factors known to increase risk and are generally developed based on experience. They can be as diverse as increasing absenteeism or increased turnover in key employees to rising levels of security events or incidents.

QUESTION 165
Risk assessment should be conducted on a continuing basis because:

A. controls change on a continuing basis
B. the number of hacking incidents is increasing
C. management should be updated about changes in risk
D. factors that affect information security change

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 166
Which of the following BEST illustrates residual risk within an organization?

A. Risk management framework
B. Risk register
C. Business impact analysis
D. Heat map

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 167
Following a recent acquisition, an information security manager has been requested to address the outstanding risk reported early in the acquisition process. Which of the following would be the manager's **BEST** course of action?

A. Add the outstanding risk to the acquiring organization's risk registry.
B. Re-assess the outstanding risk of the acquired company.
C. Re-evaluate the risk treatment plan for the outstanding risk.
D. Perform a vulnerability assessment of the acquired company's infrastructure.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 168

An organization has recently experienced unauthorized device access to its network. To proactively manage the problem and mitigate this risk, the **BEST** preventive control would be to:

A. keep an inventory of network and hardware addresses of all systems connected to the network.
B. install a stateful inspection firewall to prevent unauthorized network traffic.
C. implement network-level authentication and login to regulate access of devices to the network.
D. deploy an automated asset inventory discovery tool to identify devices that access the network.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 169
A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the **BEST** course of action to address the situation?

A. Document the deficiencies in the risk register.
B. Disconnect the legacy system from the rest of the network.
C. Require that new systems that can meet the standards be implemented.
D. Develop processes to compensate for the deficiencies.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 170
Who can BEST advocate the development of and ensure the success of an information security program?

A. Internal auditor
B. Chief operating officer (COO)
C. Steering committee
D. IT management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:
Senior management represented in the security steering committee is in the best position to advocate the establishment of and continued support for an information security program. The chief operating officer (COO) will be a member of that committee. An internal auditor is a good advocate but is secondary to the influence of senior management. IT management has a lesser degree of influence and would also be part of the steering committee.

QUESTION 171
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

A. Virtual private network (VPN)
B. Firewalls and routers
C. Biometric authentication
D. Two-factor authentication

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption of data in a virtual private network (VPN) ensures that transmitted information is not readable, even if intercepted. Firewalls and routers protect access to data resources inside the network and do not protect traffic in the public network. Biometric and two-factor authentication, by themselves, would not prevent a message from being intercepted and read.

QUESTION 172
The effectiveness of virus detection software is MOST dependent on which of the following?

A. Packet filtering
B. Intrusion detection
C. Software upgrades
D. Definition tables

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The effectiveness of virus detection software depends on virus signatures which are stored in virus definition tables. Software upgrades are related to the periodic updating of the program code, which would not be as critical. Intrusion detection and packet filtering do not focus on virus detection.

QUESTION 173
Which of the following is the MOST effective type of access control?

A. Centralized
B. Role-based
C. Decentralized
D. Discretionary

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Role-based access control allows users to be grouped into job-related categories, which significantly cases the required administrative overhead. Discretionary access control would require a greater degree of administrative overhead. Decentralized access control generally requires a greater number of staff to administer, while centralized access control is an incomplete answer.

QUESTION 174
Which of the following devices should be placed within a DMZ?

A. Router
B. Firewall
C. Mail relay
D. Authentication server

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ, network segment.

QUESTION 175
An intrusion detection system should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An intrusion detection system (IDS) should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical device.

QUESTION 176

The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

A. provide in-depth defense.
B. separate test and production.
C. permit traffic load balancing.
D. prevent a denial-of-service attack.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:
Having two entry points, each guarded by a separate firewall, is desirable to permit traffic load balancing. As they both connect to the Internet and to the same demilitarized zone (DMZ), such an arrangement is not practical for separating test from production or preventing a denial-of-service attack.

QUESTION 177
An extranet server should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

QUESTION 178
Which of the following is the BEST metric for evaluating the effectiveness of security awareness twining? The number of:

A. password resets.
B. reported incidents.
C. incidents resolved.
D. access rule violations.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Reported incidents will provide an indicator of the awareness level of staff. An increase in reported incidents could indicate that the staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. The number of incidents resolved may not correlate to staff awareness.

QUESTION 179
Security monitoring mechanisms should PRIMARILY:

A. focus on business-critical information.
B. assist owners to manage control risks.
C. focus on detecting network intrusions.
D. record all security violations.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Security monitoring must focus on business-critical information to remain effectively usable by and credible to business users. Control risk is the possibility that controls would not detect an incident or error condition, and therefore is not a correct answer because monitoring would not directly assist in managing this risk. Network intrusions are not the only focus of monitoring mechanisms; although they should record all security violations, this is not the primary objective.

QUESTION 180
Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

A. Periodic focus group meetings

B. Periodic compliance reviews
C. Computer-based certification training (CBT)
D. Employee's signed acknowledgement

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Using computer-based training (CBT) presentations with end-of-section reviews provides feedback on how well users understand what has been presented. Periodic compliance reviews are a good tool to identify problem areas but do not ensure that procedures are known or understood. Focus groups may or may not provide meaningful detail. Although a signed employee acknowledgement is good, it does not indicate whether the material has been read and/or understood.

QUESTION 181
When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

A. right-to-terminate clause.
B. limitations of liability.
C. service level agreement (SLA).
D. financial penalties clause.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Service level agreements (SLAs) provide metrics to which outsourcing firms can be held accountable. This is more important than a limitation on the outsourcing firm's liability, a right-to-terminate clause or a hold- harmless agreement which involves liabilities to third parties.

QUESTION 182
Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

A. Number of attacks detected
B. Number of successful attacks

C. Ratio of false positives to false negatives
D. Ratio of successful to unsuccessful attacks

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The ratio of false positives to false negatives will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while, at the same time, minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

QUESTION 183
Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?
A. Patch management
B. Change management
C. Security baselines
D. Virus detection

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses. Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

QUESTION 184
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart

C. Critical path
D. Rapid Application Development (RAD)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

QUESTION 185
Which of the following is MOST effective in preventing security weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Configuration management

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

QUESTION 186
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

A. calculating the residual risk.
B. enforcing the security standard.
C. redesigning the system change.
D. implementing mitigating controls.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Decisions regarding security should always weigh the potential loss from a risk against the existing controls. Each situation is unique; therefore, it is not advisable to always decide in favor of enforcing a standard. Redesigning the proposed change might not always be the best option because it might not meet the business needs. Implementing additional controls might be an option, but this would be done after the residual risk is known.

QUESTION 187

B.
Who can BEST approve plans to implement an information security governance framework?

A. Internal auditor

Information security management
C. Steering committee
D. Infrastructure management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary' to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

QUESTION 188
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

A. Baseline security standards
B. System access violation logs
C. Role-based access controls
D. Exit routines

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

C.

Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Violation logs are detective and do not prevent unauthorized access. Baseline security standards do not prevent unauthorized access. Exit routines are dependent upon appropriate role-based access.

QUESTION 189

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

A. Biometric authentication
B. Embedded steganographic
Two-factor authentication
D. Embedded digital signature

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

Explanation:

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

QUESTION 190

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. Daily
B. Weekly
C. Concurrently with O/S patch updates
D. During scheduled change control updates

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

Explanation:

D.
New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.

QUESTION 191
Which of the following devices should be placed within a demilitarized zone (DMZ)?

A. Network switch
B. Web server
C. Database server
D. File/print server

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

QUESTION 192
On which of the following should a firewall be placed?

A. Web server
B. Intrusion detection system (IDS) server
C. Screened subnet
D. Domain boundary

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A firewall should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ), does not provide any protection. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to have the firewall and the intrusion detection system (IDS) on the same physical device.

QUESTION 193
An intranet server should generally be placed on the:

A. internal network.
B. firewall server.
C. external router.
D. primary domain controller.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary- domain controllers do not normally share the physical device as the intranet server.

QUESTION 194
Access control to a sensitive intranet application by mobile users can BEST be implemented through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Two-factor authentication through the use of strong passwords combined with security tokens provides the highest level of security. Data encryption, digital signatures and strong passwords do not provide the same level of protection.

QUESTION 195
When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

A. Centralizing security management
B. Implementing sanctions for noncompliance
C. Policy enforcement by IT management
D. Periodic compliance reviews

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

By centralizing security management, the organization can ensure that security standards are applied to all systems equally and in line with established policy. Sanctions for noncompliance would not be the best way to correct poor management practices caused by work overloads or insufficient knowledge of security practices. Enforcement of policies is not solely the responsibility of IT management. Periodic compliance reviews would not correct the problems, by themselves, although reports to management would trigger corrective action such as centralizing security management.

QUESTION 196
Security awareness training is MOST likely to lead to which of the following?

A. Decrease in intrusion incidents
B. Increase in reported incidents
C. Decrease in security policy changes
D. Increase in access rule violations

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

QUESTION 197
The information classification scheme should:

A. consider possible impact of a security breach.
B. classify personal information in electronic form.
C. be performed by the information security manager.
D. classify systems according to the data processed.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Systems are not classified per se, but the data they process and store should definitely be classified.

QUESTION 198
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

A. Interoffice a system-generated complex password with 30 days expiration
B. Give a dummy password over the telephone set for immediate expiration
C. Require no password but force the user to set their own in 10 days
D. Set initial password equal to the user ID with expiration in 30 days

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Documenting the password on paper is not the best method even if sent through interoffice mail if the password is complex and difficult to memorize, the user will likely keep the printed password and this creates a security concern. A dummy (temporary) password that will need to be changed upon first logon is the best method because it is reset immediately and replaced with the user's choice of password, which will make it easier for the user to remember. If it is given to the wrong person, the legitimate user will likely notify security if still unable to access the system, so the security risk is low. Setting an account with no initial password is a security concern even if it is just for a few days. Choice D provides the greatest security threat because user IDs are typically known by both users and security staff, thus compromising access for up to 30 days.

QUESTION 199
An information security program should be sponsored by:

A. infrastructure management.
B. the corporate audit department.

C. key business process owners.
D. information security management.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The information security program should ideally be sponsored by business managers, as represented by key business process owners. Infrastructure management is not sufficiently independent and lacks the necessary knowledge regarding specific business requirements. A corporate audit department is not in as good a position to fully understand how an information security program needs to meet the needs of the business. Audit independence and objectivity will be lost, impeding traditional audit functions. Information security implements and executes the program. Although it should promote it at all levels, it cannot sponsor the effort due to insufficient operational knowledge and lack of proper authority.

QUESTION 200
Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

QUESTION 201
The BEST metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocked.
B. number of packets dropped.

C. average throughput rate.
D. number of firewall rules.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not effective measurements.

QUESTION 202
Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Acquisition management controls the purchasing process.

QUESTION 203
The MAIN advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workload.
B. increases security between multi-tier systems.
C. allows passwords to be changed less frequently.
D. reduces the need for two-factor authentication.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:
Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multi-tier systems, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

QUESTION 204
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart
C. Gap analysis
D. Balanced scorecard

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The balanced scorecard is most effective for evaluating the degree to which information security objectives are being met. A SWOT analysis addresses strengths, weaknesses, opportunities and threats. Although useful, a SWOT analysis is not as effective a tool. Similarly, a gap analysis, while useful for identifying the difference between the current state and the desired future state, is not the most appropriate tool. A waterfall chart is used to understand the flow of one process into another.

QUESTION 205
Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

A. Patch management
B. Change management
C. Security metricsD. Version control

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Change management controls the process of introducing changes to systems. Failure to have good change management may introduce new weaknesses into otherwise secure systems. Patch management corrects discovered weaknesses by applying a correction to the original program code. Security metrics provide a means for measuring effectiveness. Version control is a subset of change management.

QUESTION 206
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

A. Rewrite the application to conform to the upgraded operating system
B. Compensate for not installing the patch with mitigating controls
C. Alter the patch to allow the application to run in a privileged state
D. Run the application on a test platform; tune production to allow patch and application

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Since the operating system (OS) patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security. Since the application is critical, the patch should not be applied without regard for the application; business requirements must be considered. Altering the OS patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative since it will mean running a critical production application on a platform not subject to the same level of security controls.

QUESTION 207
Which of the following is MOST important to the success of an information security program?

A. Security' awareness training
B. Achievable goals and objectives
C. Senior management sponsorship
D. Adequate start-up budget and staffing

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Sufficient senior management support is the most important factor for the success of an information security program. Security awareness training, although important, is secondary. Achievable goals and objectives as well as having adequate budgeting and staffing are important factors, but they will not ensure success if senior management support is not present.

QUESTION 208
Which of the following is MOST important for a successful information security program?

A. Adequate training on emerging security technologies
B. Open communication with key process owners
C. Adequate policies, standards and procedures
D. Executive management commitment

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Sufficient executive management support is the most important factor for the success of an information security program. Open communication, adequate training, and good policies and procedures, while important, are not as important as support from top management; they will not ensure success if senior management support is not present.

QUESTION 209
Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

A. Screened subnets
B. Information classification policies and procedures
C. Role-based access controls
D. Intrusion detection system (IDS)

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Screened subnets are demilitarized zones (DMZs) and are oriented toward preventing attacks on an internal network by external users. The policies and procedures to classify information will ultimately result in better protection but they will not prevent actual modification. Role-based access controls would help ensure that users only had access to files and systems appropriate for their job role. Intrusion detection systems (IDS) are useful to detect invalid attempts but they will not prevent attempts.

QUESTION 210
The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

A. create more overhead than signature-based IDSs.
B. cause false positives from minor changes to system variables.
C. generate false alarms from varying user or system actions.
D. cannot detect new types of attacks.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A statistical anomaly-based intrusion detection system (stat IDS) collects data from normal traffic and establishes a baseline. It then periodically samples the network activity based on statistical methods and compares samples to the baseline. When the activity is outside the baseline parameter (clipping level), the IDS notifies the administrator. The baseline variables can include a host's memory or central processing unit (CPU) usage, network packet types and packet quantities. If actions of the users or the systems on the network vary widely with periods of low activity and periods of frantic packet exchange, a stat IDS may not be suitable, as the dramatic swing from one level to another almost certainly will generate false alarms. This weakness will have the largest impact on the operation of the IT systems. Due to the nature of stat IDS operations (i.e., they must constantly attempt to match patterns of activity to the baseline parameters), a stat IDS requires much more overhead and processing than signature-based versions. Due to the nature of a stat IDS — based on statistics and comparing data with baseline parameters — this type of IDS may not detect minor changes to system variables and may generate many false positives. Choice D is incorrect; since the stat IDS can monitor multiple system variables, it can detect new types of variables by tracing for abnormal activity of any kind.

QUESTION 211

An information security manager uses security metrics to measure the:

A. performance of the information security program.
B. performance of the security baseline.
C. effectiveness of the security risk analysis.
D. effectiveness of the incident response team.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

The security metrics should be designed so that there is a relationship to the performance of the overall security program in terms of effectiveness measurement. Use of security metrics occurs after the risk assessment process and does not measure it. Measurement of the incident response team performance is included in the overall program performance, so this is an incomplete answer.

QUESTION 212
The MOST important success factor to design an effective IT security awareness program is to:

A. customize the content to the target audience.
B. ensure senior management is represented.
C. ensure that all the staff is trained.
D. avoid technical content but give concrete examples.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Awareness training can only be effective if it is customized to the expectations and needs of attendees. Needs will be quite different depending on the target audience and will vary between business managers, end users and IT staff; program content and the level of detail communicated will therefore be different. Other criteria are also important; however, the customization of content is the most important factor.

QUESTION 213
Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

A. Use security tokens for authentication
B. Connect through an IPSec VPN
C. Use https with a server-side certificate
D. Enforce static media access control (MAC) addresses

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

IPSec effectively prevents man-in-the-middle (MitM) attacks by including source and destination IPs within the encrypted portion of the packet. The protocol is resilient to MitM attacks. Using token-based authentication does not prevent a MitM attack; however, it may help eliminate reusability of stolen cleartext credentials.
An https session can be intercepted through Domain Name Server (DNS) or Address Resolution Protocol (ARP) poisoning. ARP poisoning — a specific kind of MitM attack — may be prevented by setting static media access control (MAC) addresses. Nevertheless, DNS and NetBIOS resolution can still be attacked to deviate traffic.

QUESTION 214
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

A. Certificate-based authentication of web client
B. Certificate-based authentication of web server
C. Data confidentiality between client and web server
D. Multiple encryption algorithms

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Web browsers have the capability of authenticating through client-based certificates; nevertheless, it is not commonly used. When using https, servers always authenticate with a certificate and, once the connection is established, confidentiality will be maintained between client and server. By default, web browsers and servers support multiple encryption algorithms and negotiate the best option upon connection.

QUESTION 215
The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

A. Secure Sockets Layer (SSL).
B. Secure Shell (SSH).
C. IP Security (IPSec).
D. Secure/Multipurpose Internet Mail Extensions (S/MIME).

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet. In typical use, all data transmitted between the customer and the business are, therefore, encrypted by the business's web server and remain confidential. SSH File Transfer Protocol (SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with the SSH-2 protocol to provide secure file transfer. IP Security (IPSec) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPSec operation: transport mode and tunnel mode. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of e-mail encapsulated in MIME; it is not a web transaction protocol.

QUESTION 216
A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:

A. authentication and authorization.
B. confidentiality and integrity.

C. confidentiality and nonrepudiation.
D. authentication and nonrepudiation.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption by the private key of the sender will guarantee authentication and nonrepudiation. Encryption by the public key of the receiver will guarantee confidentiality.

QUESTION 217
When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

A. IP spoofing
B. Man-in-the-middle attack
C. Repudiation
D. Trojan

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A Trojan is a program that gives the attacker full control over the infected computer, thus allowing the attacker to hijack, copy or alter information after authentication by the user. IP spoofing will not work because IP is not used as an authentication mechanism. Man-in-the-middle attacks are not possible if using SSL with client-side certificates. Repudiation is unlikely because client-side certificates authenticate the user.

QUESTION 218
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

A. Security compliant servers trend report
B. Percentage of security compliant servers

C. Number of security patches applied
D. Security patches applied trend report

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The percentage of compliant servers will be a relevant indicator of the risk exposure of the infrastructure. However, the percentage is less relevant than the overall trend, which would provide a measurement of the efficiency of the IT security program. The number of patches applied would be less relevant, as this would depend on the number of vulnerabilities identified and patches provided by vendors.

QUESTION 219
It is important to develop an information security baseline because it helps to define:

A. critical information resources needing protection.
B. a security policy for the entire organization.

C.
the minimum acceptable security to be implemented.
D. required physical and logical access controls.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Developing an information security baseline helps to define the minimum acceptable security that will be implemented to protect the information resources in accordance with the respective criticality levels. Before determining the security baseline, an information security manager must establish the security policy, identify criticality levels of organization's information resources and assess the risk environment in which those resources operate.

QUESTION 220
Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

A. Symmetric cryptography
B. Public key infrastructure (PKI)
C. Message hashing
D. Message authentication code

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Public key infrastructure (PKI) combines public key encryption with a trusted third party to publish and revoke digital certificates that contain the public key of the sender. Senders can digitally sign a message with their private key and attach their digital certificate (provided by the trusted third party). These characteristics allow senders to provide authentication, integrity validation and nonrepudiation. Symmetric cryptography provides confidentiality. Mashing can provide integrity and confidentiality. Message authentication codes provide integrity.

QUESTION 221
Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

C.

A. Regular review of access control lists
B. Security guard escort of visitors
Visitor registry log at the door
D. A biometric coupled with a PIN

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A review of access control lists is a detective control that will enable an information security manager to ensure that authorized persons are entering in compliance with corporate policy. Visitors accompanied by a guard will also provide assurance but may not be cost effective. A visitor registry is the next cost-effective control. A biometric coupled with a PIN will strengthen the access control; however, compliance assurance logs will still have to be reviewed.

QUESTION 222
To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A. revise the information security program.
B. evaluate a balanced business scorecard.
C. conduct regular user awareness sessions.
D. perform penetration tests.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The balanced business scorecard can track the effectiveness of how an organization executes it information security strategy and determine areas of improvement. Revising the information security program may be a solution, but is not the best solution to improve alignment of the information security objectives. User awareness is just one of the areas the organization must track through the balanced business scorecard. Performing penetration tests does not affect alignment with information security objectives.

QUESTION 223

C.

What is the MOST important item to be included in an information security policy?

A. The definition of roles and responsibilities
B. The scope of the security program
The key objectives of the security program
D. Reference to procedures and standards of the security program

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Stating the objectives of the security program is the most important element to ensure alignment with business goals. The other choices are part of the security policy, but they are not as important.

QUESTION 224
In an organization, information systems security is the responsibility of:

A. all personnel.
B. information systems personnel.
C. information systems security personnel.
D. functional personnel.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

All personnel of the organization have the responsibility of ensuring information systems security-this can include indirect personnel such as physical security personnel. Information systems security cannot be the responsibility of information systems personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of information systems security personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of functional personnel alone since they cannot ensure security.

C.

QUESTION 225

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. invite an external consultant to create the security strategy.
B. allocate budget based on best practices.
C. benchmark similar organizations.

D. define high-level business security requirements.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

QUESTION 226
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

A. Number of controls
B. Cost of achieving control objectives
C. Effectiveness of controls
D. Test results of controls

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Comparison of cost of achievement of control objectives and corresponding value of assets sought to be protected would provide a sound basis for the information security manager to measure value delivery. Number of controls has no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated. Effectiveness of controls has no correlation with the value of assets unless their costs are also evaluated. Test results of controls have no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated.

QUESTION 227
Which of the following would be the BEST metric for the IT risk management process?

A. Number of risk management action plans
B. Percentage of critical assets with budgeted remedial

C. Percentage of unresolved risk exposures
D. Number of security incidents identified

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Percentage of unresolved risk exposures and the number of security incidents identified contribute to the IT risk management process, but the percentage of critical assets with budgeted remedial is the most indicative metric. Number of risk management action plans is not useful for assessing the quality of the process.

QUESTION 228
Which of the following is a key area of the ISO 27001 framework?

A. Operational risk assessment
B. Financial crime metrics
C. Capacity management
D. Business continuity management

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Operational risk assessment, financial crime metrics and capacity management can complement the information security framework, but only business continuity management is a key component.

QUESTION 229
The MAIN goal of an information security strategic plan is to:

A. develop a risk assessment plan.
B. develop a data protection plan.
C. protect information assets and resources.
D. establish security governance.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The main goal of an information security strategic plan is to protect information assets and resources. Developing a risk assessment plan and H data protection plan, and establishing security governance refer to tools utilized in the security strategic plan that achieve the protection of information assets and resources.

QUESTION 230
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

A. Encrypting first by receiver's private key and second by sender's public key
B. Encrypting first by sender's private key and second by receiver's public key
C. Encrypting first by sender's private key and second decrypting by sender's public key
D. Encrypting first by sender's public key and second by receiver's private key

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and. second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

QUESTION 231
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the system.
B. implement multifactor authentication.
C. rebuild the system from the original installation medium.

D. disconnect the mail server from the network.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

QUESTION 232
The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

A. verify the decision with the business units.
B. check the system's risk analysis.
C. recommend update after post implementation review.
D. request an audit review.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Verifying the decision with the business units is the correct answer because it is not the IT function's responsibility to decide whether a new application modifies business processes Choice B does not consider the change in the applications. Choices C and D delay the update.

QUESTION 233
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks
B. Traffic sniffing
C. Virus infections

D. IP address spoofing**Correct Answer:** B **Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation**

Explanation/Reference:
Explanation:

Network segmentation reduces the impact of traffic sniffing by limiting the amount of traffic that may be visible on any one network segment. Network segmentation would not mitigate the risk posed by denial of service (DoS) attacks, virus infections or IP address spoofing since each of these would be able to traverse network segments.

QUESTION 234
The PRIMARY objective of an Internet usage policy is to prevent:

A. access to inappropriate sites.
B. downloading malicious code.
C. violation of copyright laws.
D. disruption of Internet access.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Unavailability of Internet access would cause a business disruption. The other three objectives are secondary.

QUESTION 235
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

A. broken authentication.
B. unvalidated input.
C. cross-site scripting.
D. structured query language (SQL) injection.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

The authentication process is broken because, although the session is valid, the application should reauthenticate when the input parameters are changed. The review provided valid employee IDs, and valid input was processed. The problem here is the lack of reauthentication when the input parameters are changed. Cross-site scripting is not the problem in this case since the attack is not transferred to any other user's browser to obtain the output. Structured query language (SQL) injection is not a problem since input is provided as a valid employee ID and no SQL queries are injected to provide the output.

QUESTION 236
A test plan to validate the security controls of a new system should be developed during which phase of the project?

A. Testing
B. Initiation
C. Design
D. Development

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

In the design phase, security checkpoints are defined and a test plan is developed. The testing phase is too late since the system has already been developed and is in production testing. In the initiation phase, the basic security objective of the project is acknowledged. Development is the coding phase and is too late to consider test plans.

QUESTION 237
The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

A. service level monitoring.
B. penetration testing.
C. periodically auditing.
D. security awareness training.

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Regular audit exercise can spot any gap in the information security compliance. Service level monitoring can only pinpoint operational issues in the organization's operational environment. Penetration testing can identify security vulnerability but cannot ensure information compliance Training can increase users' awareness on the information security policy, but is not more effective than auditing.

QUESTION 238
In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

A. a strong authentication. B.
IP antispoofing filtering.
C. network encryption protocol.
D. access lists of trusted devices.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Strong authentication will provide adequate assurance on the identity of the users, while IP antispoofing is aimed at the device rather than the user. Encryption protocol ensures data confidentiality and authenticity while access lists of trusted devices are easily exploited by spoofed identity of the clients.

QUESTION 239
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

A. contribute cost-effective expertise not available internally.
B. be made responsible for meeting the security program requirements.
C. replace the dependence on internal resources.
D. deliver more effectively on account of their knowledge.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Choice A represents the primary driver for the information security manager to make use of external resources. The information security manager will continue to be responsible for meeting the security program requirements despite using the services of external resources. The external resources should never completely replace the role of internal resources from a strategic perspective. The external resources cannot have a better knowledge of the business of the information security manager's organization than do the internal resources.

QUESTION 240
Priority should be given to which of the following to ensure effective implementation of information security governance?

A. Consultation
B. Negotiation
C. Facilitation
D. Planning

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Planning is the key to effective implementation of information security governance. Consultation, negotiation and facilitation come after planning.

QUESTION 241
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. ensure the confidentiality of sensitive material.
B. provide a high assurance of identity.
C. allow deployment of the active directory.
D. implement secure sockets layer (SSL) encryption.

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The primary purpose of a public key infrastructure (PKI) is to provide strong authentication. Confidentiality is a function of the session keys distributed by the PKI. An active directory can use PKI for authentication as well as using other means. Even though secure sockets layer (SSL) encryption requires keys to authenticate, it is not the main reason for deploying PKI.

QUESTION 242
Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

A. Redundant power supplies
B. Protective switch covers
C. Shutdown alarms
D. Biometric readers

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Protective switch covers would reduce the possibility of an individual accidentally pressing the power button on a device, thereby turning off the device. Redundant power supplies would not prevent an individual from powering down a device. Shutdown alarms would be after the fact. Biometric readers would be used to control access to the systems.

QUESTION 243
Which of the following is the MOST important reason why information security objectives should be defined?

A. Tool for measuring effectiveness
B. General understanding of goals
C. Consistency with applicable standards
D. Management sign-off and support initiatives

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The creation of objectives can be used in part as a source of measurement of the effectiveness of information security management, which feeds into the overall governance. General understanding of goals and consistency with applicable standards are useful, but are not the primary reasons for having clearly defined objectives. Gaining management understanding is important, but by itself will not provide the structure for governance.

QUESTION 244
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?
A. Authentication
B. Encryption
C. Prohibit employees from copying data to USB devices
D. Limit the use of USB devices

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

QUESTION 245
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

A. an adequate budget for the security program.
B. recruitment of technical IT employees.
C. periodic risk assessments.
D. security awareness training for employees.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An information security manager has to impress upon the human resources department the need for security awareness training for all employees. Budget considerations are more of an accounting function. The human resources department would become involved once they are convinced for the need of security awareness training. Recruiting IT-savvy staff may bring in new employees with better awareness of information security, but that is not a replacement for the training requirements of the other employees. Periodic risk assessments may or may not involve the human resources department function.

QUESTION 246
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

A. Strong authentication by password
B. Encrypted hard drives
C. Multifactor authentication procedures
D. Network-based data backup

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption of the hard disks will prevent unauthorized access to the laptop even when the laptop is lost or stolen. Strong authentication by password can be bypassed by a determined hacker. Multifactor authentication can be bypassed by removal of the hard drive and insertion into another laptop. Network- based data backups do not prevent access but rather recovery from data loss.

QUESTION 247
What is the MOST important reason for conducting security awareness programs throughout an organization?

A. Reducing the human risk
B. Maintaining evidence of training records to ensure compliance
C. Informing business units about the security strategy
D. Training personnel in security incident response

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

People are the weakest link in security implementation, and awareness would reduce this risk. Through security awareness and training programs, individual employees can be informed and sensitized on various security policies and other security topics, thus ensuring compliance from each individual. Laws and regulations also aim to reduce human risk. Informing business units about the security strategy is best done through steering committee meetings or other forums.

QUESTION 248

A.

B.

At what stage of the applications development process would encryption key management initially be addressed?

Requirements development

Deployment

C. Systems testing
D. Code reviews

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption key management has to be integrated into the requirements of the application's design. During systems testing and deployment would be too late since the requirements have already been agreed upon. Code reviews are part of the final quality assurance (QA) process and would also be too late in the process.

QUESTION 249
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. messages displayed at every logon.
B. periodic security-related e-mail messages.
C. an Intranet web site for information security.
D. circulating the information security policy.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet

A.

B.

web site does not force users to access it and read the information. Circulating the information security policy atone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

QUESTION 250
Which of the following would be the BEST defense against sniffing?

Password protect the files
Implement a dynamic IP address scheme
C. Encrypt the data being transmitted
D. Set static mandatory access control (MAC) addresses

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encrypting the data will obfuscate the data so that they are not visible in plain text. Someone would have to collate the entire data stream and try decrypting it, which is not easy. Passwords can be recovered by brute-force attacks and by password crackers, so this is not the best defense against sniffing. IP addresses can always be discovered, even if dynamic IP addresses are implemented. The person sniffing traffic can initiate multiple sessions for possible IP addresses. Setting static mandatory access control (MAC) addresses can prevent address resolution protocol (ARP) poisoning, but it does not prevent sniffing.

QUESTION 251
A digital signature using a public key infrastructure (PKI) will:

A. not ensure the integrity of a message.
B. rely on the extent to which the certificate authority (CA) is trusted.
C. require two parties to the message exchange.
D. provide a high level of confidentiality.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

A.

B.

Explanation/Reference:
Explanation:

The certificate authority (CA) is a trusted third party that attests to the identity of the signatory, and reliance will be a function of the level of trust afforded the CA. A digital signature would provide a level of assurance of message integrity, but it is a three-party exchange, including the CA. Digital signatures do not require encryption of the message in order to preserve confidentiality.

QUESTION 252
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

to a higher false reject rate (FRR).

A.

B.

to a lower crossover error rate.

C. to a higher false acceptance rate (FAR).
D. exactly to the crossover error rate.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary' to reduce sensitivity and thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts — the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

QUESTION 253
Which of the following is the BEST method to securely transfer a message?

A. Password-protected removable media
B. Facsimile transmission in a secured room
C. Using public key infrastructure (PKI) encryption
D. Steganography

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Using public key infrastructure (PKI) is currently accepted as the most secure method to transmit e-mail messages. PKI assures confidentiality, integrity and nonrepudiation. The other choices are not methods that are as secure as PKI. Steganography involves hiding a message in an image.

QUESTION 254

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?

A. Monitor user activities on the network
B. Publish the standards on the intranet landing page
C. Establish an acceptable use policy
D. Deploy a device management solution

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 255
An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions house. The information security manager has determined a defense in depth strategy should be used. Which of the following **BEST** describes this strategy?

A. Multi-factor login requirements for cloud service applications, timeouts, and complex passwords
B. Deployments of nested firewalls within the infrastructure
C. Separate security controls for applications, platforms, programs, and endpoints
D. Strict enforcement of role-based access control (RBAC)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 256
When supporting an organization's privacy officer, which of the following is the information security manager's **PRIMARY** role regarding primacy requirements?

A. Monitoring the transfer of private data
B. Conducting privacy awareness programs
C. Ensuring appropriate controls are in place
D. Determining data classification

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 257
Which of the following metrics would provide management with the **MOST** useful information about the progress of a security awareness program?

A. Increased number of downloads of the organization's security policy
B. Increased reported of security incidents
C. Completion rate of user awareness training within each business unit
D. Decreased number of security incidents

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 258
An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's **FIRST** step to support this strategy?

A. Incorporate social media into the security awareness program.
B. Develop a guideline on the acceptable use of social media.
C. Develop a business case for a data loss prevention solution.
D. Employ the use of a web content filtering solution.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 259
Of the following, whose input is of GREATEST importance in the development of an information security strategy?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 260
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

A. Business impact analysis
B. Organizational risk appetite
C. Independent security audit
D. Security risk assessment

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 261
An information security manager is developing a business case for an investment in an information security control. The FIRST step should be to:

A. research vendor pricing to show cost efficiency
B. assess potential impact to the organization
C. demonstrate increased productivity of security staff
D. gain audit buy-in for the security control

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 262
Which of the following techniques would be the BEST test of security effectiveness?

A. Performing an external penetration test
B. Reviewing security policies and standards
C. Reviewing security logs
D. Analyzing technical security practices

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 263
In the event that a password policy cannot be implemented for a legacy application, which of the following is the **BEST** course of action?

A. Update the application security policy.
B. Implement compensating control.
C. Submit a waiver for the legacy application.
D. Perform an application security assessment.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 264
To ensure the information security of outsourced IT services, which of the following is the **MOST** critical due diligence activity?

A. Review samples of service level reports from the service provider.
B. Assess the level of security awareness of the service provider.
C. Request that the service provider comply with information security policy.
D. Review the security status of the service provider.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 265
Management decisions concerning information security investments will be **MOST** effective when they are based on:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 266
The contribution of recovery point objective (RPO) to disaster recovery is to:

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 267
The **BEST** way to establish a recovery time objective (RTO) that balances cost with a realistic recovery time frame is to:

A. perform a business impact analysis.
B. determine daily downtime cost.
C. analyze cost metrics.
D. conduct a risk assessment.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 268
In a large organization, defining recovery time objectives (RTOs) is **PRIMARILY** the responsibility of:

A. the IT manager.
B. the information security manager.
C. the business unit manager.
D. senior manager.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 269

Which metric is the **BEST** indicator that an update to an organization's information security awareness strategy is effective?

A. A decrease in the number of incidents reported by staff
B. A decrease in the number of email viruses detected
C. An increase in the number of email viruses detected
D. An increase in the number of incidents reported by staff

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 270

An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:

A. risk assessment results.
B. international security standards.
C. the most stringent requirements.
D. the security organization structure.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 271

Which of the following is the **PRIMARY** reason to conduct periodic business impact assessments?

A. Improve the results of last business impact assessment
B. Update recovery objectives based on new risks
C. Decrease the recovery times

D. Meet the needs of the business continuity policy

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 272
Which of the following is the **BEST** approach to make strategic information security decisions?

A. Establish an information security steering committee.
B. Establish periodic senior management meetings.
C. Establish regular information security status reporting.
D. Establish business unit security working groups.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 273
Which if the following would be the **MOST** important information to include in a business case for an information security project in a highly regulated industry?

A. Compliance risk assessment
B. Critical audit findings
C. Industry comparison analysis
D. Number of reported security incidents

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 274
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testing.
B. establish security baselines.
C. implement vendor default settings.
D. link policies to an independent standard.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security baselines will provide the best assurance that each platform meets minimum criteria. Penetration testing will not be as effective and can only be performed periodically. Vendor default settings will not necessarily meet the criteria set by the security policies, while linking policies to an independent standard will not provide assurance that the platforms meet these levels of security.

QUESTION 275
A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

A. User
B. Network
C. Operations
D. Database

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

As owners of the system, user management signoff is the most important. If a system does not meet the needs of the business, then it has not met its primary objective. The needs of network, operations and database management are secondary to the needs of the business.

QUESTION 276

The BEST way to ensure that information security policies are followed is to:

A. distribute printed copies to all employees.
B. perform periodic reviews for compliance.
C. include escalating penalties for noncompliance.
D. establish an anonymous hotline to report policy abuses.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The best way to ensure that information security policies are followed is to periodically review levels of compliance. Distributing printed copies, advertising an abuse hotline or linking policies to an international standard will not motivate individuals as much as the consequences of being found in noncompliance. Escalating penalties will first require a compliance review.

QUESTION 277
The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

A. system developer.
B. information security manager.
C. steering committee.
D. system data owner.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Data owners are the most knowledgeable of the security needs of the business application for which they are responsible. The system developer, security manager and system custodian will have specific knowledge on limited areas but will not have full knowledge of the business issues that affect the level of security required. The steering committee does not perform at that level of detail on the operation.

QUESTION 278

Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have his, her password reset?

A. Performing reviews of password resets
B. Conducting security awareness programs
C. Increasing the frequency of password changes
D. Implementing automatic password syntax checking

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Social engineering can be mitigated best through periodic security awareness training for staff members who may be the target of such an attempt. Changing the frequency of password changes, strengthening passwords and checking the number of password resets may be desirable, but they will not be as effective in reducing the likelihood of a social engineering attack.

QUESTION 279
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

A. Adequate security policies and procedures
B. Periodic compliance reviews
C. Security steering committees
D. Security awareness campaigns

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security awareness campaigns will be more effective at changing an organizational culture than the creation of steering committees and security policies and procedures. Compliance reviews are helpful; however, awareness by all staff is more effective because compliance reviews are focused on certain areas groups and do not necessarily educate.

QUESTION 280

The BEST way to ensure that an external service provider complies with organizational security policies is to:

A. Explicitly include the service provider in the security policies.

B. Receive acknowledgment in writing stating the provider has read all policies.
C. Cross-reference to policies in the service level agreement
D. Perform periodic reviews of the service provider.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Periodic reviews will be the most effective way of obtaining compliance from the external service provider. References in policies and service level agreements and requesting written acknowledgement will not be as effective since they will not trigger the detection of noncompliance.

QUESTION 281
When an emergency security patch is received via electronic mail, the patch should FIRST be:

A. loaded onto an isolated test machine.
B. decompiled to check for malicious code.
C. validated to ensure its authenticity.
D. copied onto write-once media to prevent tampering.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is important to first validate that the patch is authentic. Only then should it be copied onto write-once media, decompiled to check for malicious code or loaded onto an isolated test machine.

QUESTION 282
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security software will generally have a well-controlled process for applying patches, backing up files and upgrading hardware. The greatest risk occurs when access rules are changed since they are susceptible to being opened up too much, which can result in the creation of a security exposure.

QUESTION 283
Which of the following is the BEST indicator that security awareness training has been effective?

A. Employees sign to acknowledge the security policy
B. More incidents are being reported
C. A majority of employees have completed training
D. No incidents have been reported in three months

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

More incidents being reported could be an indicator that the staff is paying more attention to security. Employee signatures and training completion may or may not have anything to do with awareness levels. The number of individuals trained may not indicate they are more aware. No recent security incidents do not reflect awareness levels, but may prompt further research to confirm.

QUESTION 284
Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs?

A. Penetration attempts investigated
B. Violation log reports produced

C. Violation log entries
D. Frequency of corrective actions taken

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The most useful metric is one that measures the degree to which complete follow-through has taken place. The quantity of reports, entries on reports and the frequency of corrective actions are not indicative of whether or not investigative action was taken.

QUESTION 285
Which of the following change management activities would be a clear indicator that normal operational procedures require examination? A high percentage of:

A. similar change requests.
B. change request postponements.
C. canceled change requests.
D. emergency change requests.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A high percentage of emergency change requests could be caused by changes that are being introduced at the last minute to bypass normal chance management procedures. Similar requests, postponements and canceled requests all are indicative of a properly functioning change management process.

QUESTION 286
Which of the following is the MOST important management signoff for migrating an order processing system from a test environment to a production environment?

A. User
B. Security
C. Operations
D. Database

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
As owners of the system, user management approval would be the most important. Although the signoffs of security, operations and database management may be appropriate, they are secondary to ensuring the new system meets the requirements of the business.

QUESTION 287
Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

A. the third party provides a demonstration on a test system.
B. goals and objectives are clearly defined.
C. the technical staff has been briefed on what to expect.
D. special backups of production servers are taken.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The most important action is to clearly define the goals and objectives of the test. Assuming that adequate backup procedures are in place, special backups should not be necessary. Technical staff should not be briefed nor should there be a demo as this will reduce the spontaneity of the test.

QUESTION 288
When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

A. submit the issue to the steering committee.
B. conduct an impact analysis to quantify the risks.
C. isolate the system from the rest of the network.
D. request a risk acceptance from senior management.

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

An impact analysis is warranted to determine whether a risk acceptance should be granted and to demonstrate to the department the danger of deviating from the established policy. Isolating the system would not support the needs of the business. Any waiver should be granted only after performing an impact analysis.

QUESTION 289
Which of the following is MOST important to the successful promotion of good security management practices?

A. Security metrics
B. Security baselines
C. Management support
D. Periodic training

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Without management support, all other efforts will be undermined. Metrics, baselines and training are all important, but they depend on management support for their success.

QUESTION 290
Which of the following environments represents the GREATEST risk to organizational security?

A. Locally managed file server
B. Enterprise data warehouse
C. Load-balanced, web server cluster
D. Centrally managed data switch

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A locally managed file server will be the least likely to conform to organizational security policies because it is generally subject to less oversight and monitoring. Centrally managed data switches, web server clusters and data warehouses are subject to close scrutiny, good change control practices and monitoring.

QUESTION 291
Nonrepudiation can BEST be assured by using:
A. delivery path tracing.
B. reverse lookup translation.
C. out-of-hand channels.
D. digital signatures.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Effective nonrepudiation requires the use of digital signatures. Reverse lookup translation involves converting Internet Protocol (IP) addresses to usernames. Delivery path tracing shows the route taken but does not confirm the identity of the sender. Out-of-band channels are useful when, for confidentiality, it is necessary to break a message into two parts that are sent by different means.

QUESTION 292
Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

A. mandatory access controls.
B. discretionary access controls.C. lattice-based access controls.
D. role-based access controls.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Role-based access controls will grant temporary employee access based on the job function to be performed. This provides a better means of ensuring that the access is not more or less than what is required. Discretionary, mandatory and lattice-based access controls are all security models, hut they do not address the issue of temporary employees as well as role-based access controls.

QUESTION 293
Which of the following areas is MOST susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management C. Configuration management
D. Incident response management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Configuration management provides the greatest likelihood of security weaknesses through misconfiguration and failure to update operating system (OS) code correctly and on a timely basis.

QUESTION 294
Security policies should be aligned MOST closely with:

A. industry' best practices.
B. organizational needs.
C. generally accepted standards.
D. local laws and regulations.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The needs of the organization should always take precedence. Best practices and local regulations are important, but they do not take into account the total needs of an organization.

QUESTION 295
The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performance.
B. use a honeypot to check for unusual activity.
C. audit the configuration of the IDS.
D. benchmark the IDS against a peer site.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Simulating an attack on the network demonstrates whether the intrusion detection system (IDS) is properly tuned. Reviewing the configuration may or may not reveal weaknesses since an anomaly-based system uses trends to identify potential attacks. A honeypot is not a good first step since it would need to have already been penetrated. Benchmarking against a peer site would generally not be practical or useful.

QUESTION 296
The BEST time to perform a penetration test is after:

A. an attempted penetration has occurred.
B. an audit has reported weaknesses in security controls.
C. various infrastructure changes are made.
D. a high turnover in systems staff.

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Changes in the systems infrastructure are most likely to inadvertently introduce new exposures. Conducting a test after an attempted penetration is not as productive since an organization should not wait until it is attacked to test its defenses. Any exposure identified by an audit should be corrected before it would be appropriate to test. A turnover in administrative staff does not warrant a penetration test, although it may- warrant a review of password change practices and configuration management.

QUESTION 297
Successful social engineering attacks can BEST be prevented through:
A. preemployment screening.
B. close monitoring of users' access patterns.
C. periodic awareness training.
D. efficient termination procedures.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

QUESTION 298
What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

A. Perform periodic penetration testing
B. Establish minimum security baselines
C. Implement vendor default settings
D. Install a honeypot on the network

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed sporadically. Vendor default settings are not effective.

QUESTION 299
Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

A. User ad hoc reporting is not logged

B. Network traffic is through a single switch
C. Operating system (OS) security patches have not been applied
D. Database security defaults to ERP settings

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security-weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

QUESTION 300
In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

A. Implementing on-screen masking of passwords
B. Conducting periodic security awareness programs
C. Increasing the frequency of password changes
D. Requiring that passwords be kept strictly confidential

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt. Implementing on-screen masking of passwords and increasing the frequency of password changes are desirable, but these will not be effective in reducing the likelihood of a successful social engineering attack. Requiring that passwords be kept secret in security policies is a good control but is not as effective as periodic security awareness programs that will alert users of the dangers posed by social engineering.

QUESTION 301
Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security-steering committees
D. Security awareness campaigns

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self- assessment exercises are all good but do not exemplify the taking of ownership by management.

QUESTION 302
Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System analyst
B. Quality control manager
C. Process owner
D. Information security manager

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

QUESTION 303
What is the BEST way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards
B. Have the contractors acknowledge in writing the security policies
C. Create penalties for noncompliance in the contracting agreement
D. Perform periodic security reviews of the contractors

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Periodic reviews are the most effective way of obtaining compliance. None of the other options detects the failure of contract programmers to comply.

QUESTION 304
Which of the following activities is MOST likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

If malicious code is not immediately detected, it will most likely be backed up as a part of the normal tape backup process. When later discovered, the code may be eradicated from the device but still remain undetected ON a backup tape. Any subsequent restores using that tape may reintroduce the malicious code. Applying patches, changing access rules and upgrading hardware does not significantly increase the level of difficulty.

QUESTION 305
Security awareness training should be provided to new employees:

A. on an as-needed basis.
B. during system user training.
C. before they have access to data.
D. along with department staff.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security awareness training should occur before access is granted to ensure the new employee understands that security is part of the system and business process. All other choices imply that security awareness training is delivered subsequent to the granting of system access, which may place security as a secondary step.

QUESTION 306
What is the BEST method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to operating system (OS) patch logs
B. Trace OS patch logs to OS vendor's update documentation
C. Trace OS patch logs to change control requests
D. Review change control documentation for key servers

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

To ensure that all patches applied went through the change control process, it is necessary to use the operating system (OS) patch logs as a starting point and then check to see if change control documents are on file for each of these changes. Tracing from the documentation to the patch log will not indicate if some patches were applied without being documented. Similarly, reviewing change control documents for key servers or comparing patches applied to those recommended by the OS vendor's web site does not confirm that these security patches were properly approved and documented.

QUESTION 307
A security awareness program should:

A. present top management's perspective.
B. address details on specific exploits.
C. address specific groups and roles.
D. promote security department procedures.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Different groups of employees have different levels of technical understanding and need awareness training that is customized to their needs; it should not be presented from a specific perspective. Specific details on technical exploits should be avoided since this may provide individuals with knowledge they might misuse or it may confuse the audience. This is also not the best forum in which to present security department procedures.

QUESTION 308
The PRIMARY objective of security awareness is to:

A. ensure that security policies are understood.
B. influence employee behavior.
C. ensure legal and regulatory compliance
D. notify of actions for noncompliance.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, or meeting legal and regulatory requirements is important but secondary.

QUESTION 309
Which of the following will BEST protect against malicious activity by a former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:
Explanation:

When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important, but are not as effective in preventing this type of situation.

QUESTION 310
In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

A. testing time window prior to deployment.
B. technical skills of the team responsible.
C. certification of validity for deployment.
D. automated deployment to all the servers.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Having the patch tested prior to implementation on critical systems is an absolute prerequisite where availability is a primary concern because deploying patches that could cause a system to fail could be worse than the vulnerability corrected by the patch. It makes no sense to deploy patches on every system. Vulnerable systems should be the only candidate for patching. Patching skills are not required since patches are more often applied via automated tools.

QUESTION 311
To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

A. end users.
B. legal counsel.
C. operational units.
D. audit management.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
Procedures at the operational level must be developed by or with the involvement of operational units that will use them. This will ensure that they are functional and accurate. End users and legal counsel are normally not involved in procedure development. Audit management generally oversees information security operations but does not get involved at the procedural level.

QUESTION 312
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The research and development department is usually the most sensitive area of the pharmaceutical organization, Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical: therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

QUESTION 313
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

A. The program's governance oversight mechanisms
B. Information security periodicals and manuals
C. The program's security architecture and design
D. Training and certification of the information security team

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
While choices B, C and D will all assist the currency and coverage of the program, its governance oversight mechanisms are the best method.

QUESTION 314
Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

A. Security audit reports
B. Balanced scorecard
C. Capability maturity model (CMM)
D. Systems and business security architecture

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The capability maturity model (CMM) grades each defined area of security processes on a scale of 0 to 5 based on their maturity, and is commonly used by entities to measure their existing state and then determine the desired one. Security audit reports offer a limited view of the current state of security. Balanced scorecard is a document that enables management to measure the implementation of their strategy and assists in its translation into action. Systems and business security architecture explain the security architecture of an entity in terms of business strategy, objectives, relationships, risks, constraints and enablers, and provides a business-driven and business-focused view of security architecture.

QUESTION 315
Who is responsible for raising awareness of the need for adequate funding for risk action plans?

A. Chief information officer (CIO)
B. Chief financial officer (CFO)
C. Information security manager
D. Business unit management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The information security manager is responsible for raising awareness of the need for adequate funding for risk-related action plans. Even though the chief information officer (CIO), chief financial officer (CFO) and business unit management are involved in the final approval of fund expenditure, it is the information security manager who has the ultimate responsibility for raising awareness.

QUESTION 316
Managing the life cycle of a digital certificate is a role of a(n):

A. system administrator.
B. security administrator.
C. system developer.
D. independent trusted source.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Digital certificates must be managed by an independent trusted source in order to maintain trust in their authenticity. The other options are not necessarily entrusted with this capability.

QUESTION 317
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

A. Budget allocation
B. Technical skills of staff
C. User acceptance
D. Password requirements

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

End users may react differently to the implementation, and may have specific preferences. The information security manager should be aware that what is viewed as reasonable in one culture may not be acceptable in another culture. Budget allocation will have a lesser impact since what is rejected as a result of culture cannot be successfully implemented regardless of budgetary considerations. Technical skills of staff will have a lesser impact since new staff can be recruited or existing staff can be trained. Although important, password requirements would be less likely to guarantee the success of the implementation.

QUESTION 318
Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

A. Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans
B. Periodic audits of the disaster recovery/business continuity plans
C. Comprehensive walk-through testing
D. Inclusion as a required step in the system life cycle process

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information security should be an integral component of the development cycle; thus, it should be included at the process level. Choices A, B and C are good mechanisms to ensure compliance, but would not be nearly as timely in ensuring that the plans are always up-to-date. Choice D is a preventive control, while choices A, B and C are detective controls.

QUESTION 319
When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/ disaster recovery plans is because:

A. this is a requirement of the security policy.
B. software licenses may expire in the future without warning.
C. the asset inventory must be maintained.
D. service level agreements may not otherwise be met.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The key requirement is to preserve availability of business operations. Choice A is a correct compliance requirement, but is not the main objective in this case. Choices B and C are supplementary requirements for business continuity/disaster recovery planning.

QUESTION 320
To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

A. Service level agreements (SLAs)
B. Right to audit clause
C. Intrusion detection system (IDS) services
D. Spam filtering services

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Service level agreements (SLA) will be most effective in ensuring that Internet service providers (ISPs) comply with expectations for service availability. Intrusion detection system (IDS) and spam filtering services would not mitigate (as directly) the potential for service interruptions. A right-to-audit clause would not be effective in mitigating the likelihood of a service interruption.

QUESTION 321
To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

A. create a separate account for the programmer as a power user.
B. log all of the programmers' activity for review by supervisor.
C. have the programmer sign a letter accepting full responsibility.
D. perform regular audits of the application.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers' actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

QUESTION 322
Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

A. are compatible with the provider's own classification.
B. are communicated to the provider.
C. exceed those of the outsourcer.
D. are stated in the contract.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A. B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

QUESTION 323
What is the GREATEST risk when there is an excessive number of firewall rules?

A. One rule may override another rule in the chain and create a loophole
B. Performance degradation of the whole network
C. The firewall may not support the increasing number of rules due to limitations
D. The firewall may show abnormal behavior and may crash or automatically shut down

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

If there are many firewall rules, there is a chance that a particular rule may allow an external connection although other associated rules are overridden. Due to the increasing number of rules, it becomes complex to test them and. over time, a loophole may occur.

QUESTION 324
Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?
A. Mantrap
B. Biometric lock
C. Closed-circuit television (CCTV)
D. Security guard

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

QUESTION 325
What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

A. Provide detailed instructions on how to carry out different types of tasks
B. Ensure consistency of activities to provide a more stable environment
C. Ensure compliance to security standards and regulatory requirements
D. Ensure reusability to meet compliance to quality requirements

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Developing procedures and guidelines to ensure that business processes address information security risk is critical to the management of an information security program. Developing procedures and guidelines establishes a baseline for security program performance and consistency of security activities.

QUESTION 326
What is the BEST way to ensure data protection upon termination of employment?

A. Retrieve identification badge and card keys
B. Retrieve all personal computer equipment
C. Erase all of the employee's folders

D.
Ensure all logical access is removed

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Ensuring all logical access is removed will guarantee that the former employee will not be able to access company data and that the employee's credentials will not be misused. Retrieving identification badge and card keys would only reduce the capability to enter the building. Retrieving the personal computer equipment and the employee's folders are necessary tasks, but that should be done as a second step.

QUESTION 327
The MOST important reason for formally documenting security procedures is to ensure:

A. processes are repeatable and sustainable.
B. alignment with business objectives.
C. auditability by regulatory agencies.
D. objective criteria for the application of metrics.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Without formal documentation, it would be difficult to ensure that security processes are performed in the proper manner every time that they are performed. Alignment with business objectives is not a function of formally documenting security procedures. Processes should not be formally documented merely to satisfy an audit requirement. Although potentially useful in the development of metrics, creating formal documentation to assist in the creation of metrics is a secondary objective.

QUESTION 328
Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

A. Conduct awareness sessions on intellectual property policy

D.
B. Require all employees to sign a nondisclosure agreement
C. Promptly remove all access when an employee leaves the organization
Restrict access to a need-to-know basis

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security awareness regarding intellectual property policy will not prevent violations of this policy. Requiring all employees to sign a nondisclosure agreement and promptly removing all access when an employee leaves the organization are good controls, but not as effective as restricting access to a need-to- know basis.

QUESTION 329
The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

A. Data owner
B. Data custodian
C. Systems programmer
D. Security administrator

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A systems programmer should not have privileges to modify the access control list (ACL) because this would give the programmer unlimited control over the system. The data owner would request and approve updates to the ACL, but it is not a violation of the separation of duties principle if the data owner has update rights to the ACL. The data custodian and the security administrator could carry out the updates on the ACL since it is part of their duties as delegated to them by the data owner.

QUESTION 330

D.
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
Require that a change request be submitted for each download

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Administrative accounts have permission to change data. This is not required for the developers to perform their tasks. Unauthorized change will damage the integrity of the data. Logging all usage of the account, suspending the account and activating only when needed, and requiring that a change request be submitted for each download will not reduce the exposure created by this excessive level of access. Restricting the account to read only access will ensure that the integrity can be maintained while permitting access.

QUESTION 331
Which would be the BEST recommendation to protect against phishing attacks?

A. Install an antispam system
B. Publish security guidance for customers
C. Provide security awareness to the organization's staff

D.
D. Install an application-level firewall

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Customers of the organization are the target of phishing attacks. Installing security software or training the organization's staff will be useless. The effort should be put on the customer side.

QUESTION 332
Which of the following is the BEST indicator that an effective security control is built into an organization?

A. The monthly service level statistics indicate a minimal impact from security issues.
B. The cost of implementing a security control is less than the value of the assets.
C. The percentage of systems that is compliant with security standards.
D. The audit reports do not reflect any significant findings on security.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The best indicator of effective security control is the evidence of little disruption to business operations. Choices B, C and D can support this evidence, but are supplemental to choice A.

QUESTION 333
What is the BEST way to alleviate security team understaffing while retaining the capability in-house?

A. Hire a contractor that would not be included in the permanent headcount
B. Outsource with a security services provider while retaining the control internally
C. Establish a virtual security team from competent employees across the company
D. Provide cross training to minimize the existing resources gap

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

While hiring an indirect resource that will not be part of headcount will help to add an extra resource, it usually costs more than a direct employee; thus, it is not cost efficient. Outsourcing may be a more expensive option and can add complexities to the service delivery. Competent security staff can be recruited from other departments e.g., IT. product development, research and development (R&D). By leveraging existing resources, there is a nominal additional cost. It is also a strategic option since the staff may join the team as full members in the future (internal transfer). Development of staff is often a budget drain and, if not managed carefully, these resources may move away from the company and leave the team with a bigger resource gap.

QUESTION 334
When developing security standards, which of the following would be MOST appropriate to include?

A. Accountability for licenses
B. Acceptable use of IT assets
C. operating system requirements
D. Inventory management

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 335
Which of the following would be MOST effective in the strategic alignment of security initiatives?

A. A security steering committee is set up within the IT department.
B. Key information security policies are updated on a regular basis.
C. Business leaders participate in information security decision making.
D. Policies are created with input from business unit managers.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 336
Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Ensure that proper controls exist for code review and release management
B. Set up an agent to run a virus-scanning program across platforms
C. Implement controls for continuous monitoring of middleware transactions
D. Apply the latest patch programs to the production operating systems

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 337
The BEST way to mitigate the risk associated with a social engineering attack is to:

A. deploy an effective intrusion detection system (IDS)
B. perform a user-knowledge gap assessment of information security practices
C. perform a business risk assessment of the email filtering system
D. implement multi-factor authentication on critical business systems

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 338
When considering whether to adopt a new information security framework, an organization's information security manager should FIRST:

A. compare the framework with the current business strategy
B. perform a technical feasibility analysis
C. perform a financial viability study
D. analyze the framework's legal implications and business impact

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 339

A data-hosting organization's data center houses servers, applications, and data for a large number of geographically dispersed customers. Which of the following strategies would be the BEST approach for developing a physical access control policy for the organization?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 340
After detecting an advanced persistent threat (APT), which of the following should be the information security manager's FIRST step?

A. Notify management
B. Contain the threat
C. Remove the threat
D. Perform root-cause analysis

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 341
A new system has been developed that does not comply with password-aging rules. This noncompliance can BEST be identified through:

A. a business impact analysis
B. an internal audit assessment
C. an incident management process
D. a progressive series of warnings

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 342
Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

A. Client logins are subject to replay attack
B. Compromised VPN clients could impact the network
C. Attackers could compromise the VPN gateway
D. VPN traffic could be sniffed and captured

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Reference *https://resources.infosecinstitute.com/importance-effective-vpn-remote-access-policy/#gref*

QUESTION 343
In which of the following ways can an information security manager BEST ensure that security controls are adequate for supporting business goals and objectives?

A. Reviewing results of the annual company external audit
B. Adopting internationally accepted controls
C. Enforcing strict disciplinary procedures in case of noncompliance
D. Using the risk management process

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 344
The authorization to transfer the handling of an internal security incident to a third-party support provider is PRIMARILY defined by the:

A. information security manager
B. escalation procedures
C. disaster recovery plan
D. chain of custody

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 345
Which of the following outsourced services has the GREATEST need for security monitoring?

A. Enterprise infrastructure
B. Application development
C. Virtual private network (VPN) services
D. Web site hosting

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 346
Which of the following is done PRIMARILY to address the integrity of information?

A. Assignment of appropriate control permissions
B. Implementation of an Internet security application
C. Implementation of a duplex server system
D. Encryption of email

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 347
An organization has a policy in which all criminal activity is prosecuted. What is MOST important for the information security manager to ensure when an employee is suspected of using a company computer to commit fraud?

A. The forensics process is immediately initiated
B. The incident response plan is initiated
C. The employee's log files are backed-up
D. Senior management is informed of the situation

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 348
A multinational organization's information security manager has been advised that the city in which a contracted regional data center is located is experiencing civil unrest. The information security manager should FIRST:

A. delete the organization's sensitive data at the provider's location
B. engage another service provider at a safer location
C. verify the provider's ability to protect the organization's data
D. evaluate options to recover if the data center becomes unreachable

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 349
When defining responsibilities with a cloud computing vendor, which of the following should be regarded as a shared responsibility between user and provider?

A. Data ownership
B. Access log review
C. Application logging
D. Incident response

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 350
An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:

A. map the strategy to business objectives
B. perform a cost-benefit analysis
C. conduct a risk assessment
D. develop a business case

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 351
A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

A. change the password policy to improve the customer experience
B. research alternative secure methods of identity verification
C. evaluate the impact of the customer's experience on business revenue
D. recommend implementing two-factor authentication

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 352
The PRIMARY reason for creating a business case when proposing an information security project is to:

A. establish the value of the project in relation to business objectives
B. establish the value of the project with regard to regulatory compliance
C. ensure relevant business parties are involved in the project
D. ensure comprehensive security controls are identified

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 353
Which of the following will BEST help to proactively prevent the exploitation of vulnerabilities in operating system software?

A. Patch management
B. Threat management
C. Intrusion detection system
D. Anti-virus software

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 354
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. Requiring the backup of the organization's data by the user
B. Establishing the authority to remote wipe
C. Monitoring how often the smartphone is used
D. Developing security awareness training

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 355
During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

A. Eradication
B. Review
C. Containment
D. Identification

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 356
Employees in a large multinational organization frequently travel among various geographic locations. Which type of authorization policy **BEST** addresses this practice?

A. Multilevel
B. Identity
C. Role-based
D. Discretionary

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 357
To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:

A. assess security during equipment deployment.
B. ensure compliance during user acceptance testing.
C. assess the risks of all new equipment.
D. develop an approved equipment list.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 358
Segregation of duties is a security control **PRIMARILY** used to:

A. establish dual check.
B. establish hierarchy.
C. limit malicious behavior.
D. decentralize operations.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 359
Which of the following is the BEST approach when using sensitive customer data during the testing phase of a systems development project?

A. Establish the test environment on a separate network.

B. Sanitize customer data.
C. Monitor the test environment for data loss.
D. Implement equivalent controls to those on the source system.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 360
Without prior approval, a training department enrolled the company in a free cloud-based collaboration site and invited employees to use it. Which of the following is the **BEST** response of the information security manager?

A. Conduct a risk assessment and develop an impact analysis.
B. Update the risk register and review the information security strategy.
C. Report the activity to senior management.
D. Allow temporary use of the site and monitor for data leakage.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 361
A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is **MOST** important to ensure:

A. data sharing complies with local laws and regulations at both locations.
B. data is encrypted in transit and at rest.
C. a nondisclosure agreement is signed.
D. risk coverage is split between the two locations sharing data.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 362
Which of the following is **MOST** likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

A. The activities being monitored deviate from what is considered normal.
B. The information regarding monitored activities becomes stale.
C. The pattern of normal behavior changes quickly and dramatically.
D. The environment is complex.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 363
An information security manager is reviewing the impact of a regulation on the organization's human resources system. The **NEXT** course of action should be to:

A. perform a gap analysis of compliance requirements.
B. assess the penalties for non-compliance.
C. review the organization's most recent audit report.
D. determine the cost of compliance.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 364
Which of the following will **BEST** protect confidential data when connecting large wireless networks to an existing wired-network infrastructure?

A. Mandatory access control (MAC) address filtering

B. Strong passwords
C. Virtual private network (VPN)
D. Firewall

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 365
A global organization processes and stores large volumes of personal data. Which of the following would be the MOST important attribute in creating a data access policy?

A. Availability
B. Integrity
C. Reliability
D. Confidentiality

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 366
An organization to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

A. Evaluate the cost of information security integration
B. Assess the business objectives of the processes
C. Identify information security risk associated with the processes
D. Benchmark the processes with best practice to identify gaps

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 367

Which of the following is MOST important for an information security manager to regularly report to senior management?

A. Results of penetration tests
B. Audit reports
C. Impact of unremediated risks
D. Threat analysis reports

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 368

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 369
Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?
A. Warm
B. Redundant
C. Shared
D. Mobile

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Reference https://searchdisasterrecovery.techtarget.com/answer/Whats-the-difference-between-a-hot-site-and-cold-site-for-disaster-recovery

QUESTION 370
Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

A. Effective security eliminates risk to the business
B. Adopt a recognized framework with metrics
C. Security is a business product and not a process
D. Security supports and protects the business

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 371
Which of the following characteristics is MOST important to a bank in a high-value online financial transaction system?

A. Identification
B. Confidentiality
C. Authentication

D. Audit monitoring

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 372
Which of the following presents the GREATEST challenge in calculating return on investment (ROI) in the security environment?

A. Number of incidents cannot be predetermined
B. Project cost overruns cannot be anticipated
C. Cost of security tools is difficult to estimate
D. Costs of security incidents cannot be estimated

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 373
Which of the following would MOST likely require a business continuity plan to be invoked?

A. An unauthorized visitor discovered in the data center
B. A distributed denial of service attack on an e-mail server
C. An epidemic preventing staff from performing job functions
D. A hacker holding personally identifiable information hostage

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 374

Which of the following is the **MOST** important driver when developing an effective information security strategy?

A. Information security standards
B. Compliance requirements
C. Benchmark reports
D. Security audit reports

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 375

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

A. Business impact if threats materialize
B. Availability of unused funds in the security budget
C. Threat information from reputable sources
D. Alignment of the new initiative with the approved business strategy

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 376

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

A. An intrusion detection system
B. Established security baselines
C. Penetration testing

D. Log aggregation and correlation

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 377
When messages are encrypted and digitally signed to protect documents transferred between trading partners, the **GREATEST** concern is that:

A. trading partners can repudiate the transmission of messages.
B. hackers can eavesdrop on messages.
C. trading partners can repudiate the receipt of messages.
D. hackers can introduce forgery messages.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 378
Which of the following should be determined FIRST when establishing a business continuity program?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION 379
A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. disconnecting the computer from all power sources.
B. disabling all local user accounts except for one administrator.
C. encrypting local files and uploading exact copies to a secure server.
D. copying all files using the operating system (OS) to write-once media.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing it remotely changes the operating system (OS) and temporary files on the computer and invalidates it as admissible evidence.

QUESTION 380
A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GREATEST weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks
B. The hot site may have to be shared with other customers
C. The time of declaration determines site access priority
D. The provider services all major companies in the area

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. Access to a hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

QUESTION 381
Which of the following actions should be taken when an online trading company discovers a network attack in progress?
A. Shut off all network access points
B. Dump all event logs to removable media
C. Isolate the affected network segment
D. Enable trace logging on all event

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

QUESTION 382
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.
B. bastion hosts.
C. decoy files.
D. screened subnets.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

QUESTION 383
What is the PRIMARY objective of a post-event review in incident response?

A. Adjust budget provisioning
B. Preserve forensic data
C. Improve the response process
D. Ensure the incident is fully documented

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The primary objective is to find any weakness in the current process and improve it. The other choices are all secondary.

QUESTION 384
Detailed business continuity plans should be based PRIMARILY on:

A. consideration of different alternatives.
B. the solution that is least expensive.
C. strategies that cover all applications.
D. strategies validated by senior management.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

A recovery strategy identifies the best way to recover a system in ease of disaster and provides guidance based on detailed recovery procedures that can be developed. Different strategies should be developed and all alternatives presented to senior management. Senior management should select the most appropriate

strategy from the alternatives provided. The selected strategy should be used for further development of the detailed business continuity plan. The selection of strategy depends on criticality of the business process and applications supporting the processes. It need not necessarily cover all applications. All recovery strategies have associated costs, which include costs of preparing for disruptions and putting them to use in the event of a disruption. The latter can be insured against, but not the former. The best recovery option need not be the least expensive.

QUESTION 385
A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. rebuild the server from the last verified backup.
B. place the web server in quarantine.
C. shut down the server in an organized manner.
D. rebuild the server with original media and relevant patches.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

QUESTION 386
Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

A. A bit-level copy of all hard drive data
B. The last verified backup stored offsite
C. Data from volatile memory
D. Backup servers

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The bit-level copy image file ensures forensic quality evidence that is admissible in a court of law. Choices B and D may not provide forensic quality data for investigative work, while choice C alone may not provide enough evidence.

QUESTION 387
In the course of responding 10 an information security incident, the BEST way to treat evidence for possible legal action is defined by:

A. international standards.
B. local regulations.
C. generally accepted best practices.
D. organizational security policies.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Legal follow-up will most likely be performed locally where the incident took place; therefore, it is critical that the procedure of treating evidence is in compliance with local regulations. In certain countries, there are strict regulations on what information can be collected. When evidence collected is not in compliance with local regulations, it may not be admissible in court. There are no common regulations to treat computer evidence that are accepted internationally. Generally accepted best practices such as a common chain-of-custody concept may have different implementation in different countries, and thus may not be a good assurance that evidence will be admissible. Local regulations always take precedence over organizational security policies.

QUESTION 388
Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

A. determining the extent of property damage.
B. preserving environmental conditions.
C. ensuring orderly plan activation.
D. reducing the extent of operational damage.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

During an incident, emergency actions should minimize or eliminate casualties and damage to the business operation, thus reducing business interruptions. Determining the extent of property damage is not the consideration; emergency actions should minimize, not determine, the extent of the damage. Protecting/ preserving environmental conditions may not be relevant. Ensuring orderly plan activation is important but not as critical as reducing damage to the operation.

QUESTION 389
What is the FIRST action an information security manager should take when a company laptop is reported stolen?

A. Evaluate the impact of the information loss
B. Update the corporate laptop inventory
C. Ensure compliance with reporting procedures
D. Disable the user account immediately

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The key step in such an incident is to report it to mitigate any loss. After this, the other actions should follow.

QUESTION 390
When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

A. services delivery objective.
B. recovery time objective (RTO).
C. recovery window.
D. maximum tolerable outage (MTO).

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The length of the recovery window is defined by business management and determines the acceptable time frame between a disaster and the restoration of critical services/applications. The technical implementation of the disaster recovery (DR) site will be based on this constraint, especially the choice between a hot, warm or cold site. The service delivery objective is supported during the alternate process mode until the normal situation is restored, which is directly related to business needs. The recovery time objective (RTO) is commonly agreed to be the time frame between a disaster and the return to normal operations. It is then longer than the interruption window and is very difficult to estimate in advance. The time frame between the reduced operation mode at the end of the interruption window and the return to normal operations depends on the magnitude of the disaster. Technical disaster recovery solutions alone will not be used for returning to normal operations. Maximum tolerable outage (MTO) is the maximum time acceptable by a company operating in reduced mode before experiencing losses. Theoretically, recovery time objectives (RTOs) equal the interruption window plus the maximum tolerable outage. This will not be the primary factor for the choice of the technical disaster recovery solution.

QUESTION 391

In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

A.
volume of sensitive data.
B. recovery point objective (RPO).
C. recovery' time objective (RTO).
D. interruption window.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The recovery point objective (RPO) defines the maximum loss of data (in terms of time) acceptable by the business (i.e., age of data to be restored). It will directly determine the basic elements of the backup strategy frequency of the backups and what kind of backup is the most appropriate (disk-to-disk, on tape, mirroring). The volume of data will be used to determine the capacity of the backup solution. The recovery time objective (RTO) — the time between disaster and return to normal operation — will not have any impact on the backup strategy. The availability to restore backups in a time frame consistent with the interruption window will have to be checked and will influence the strategy (e.g., full backup vs. incremental), but this will not be the primary factor.

QUESTION 392
An intrusion detection system (IDS) should:

A. run continuously
B. ignore anomalies
C. require a stable, rarely changed environment
D. be located on the network

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

If an intrusion detection system (IDS) does not run continuously the business remains vulnerable. An IDS should detect, not ignore anomalies. An IDS should be flexible enough to cope with a changing environment. Both host and network based IDS are recommended for adequate detection.

QUESTION 393

A.
The PRIORITY action to be taken when a server is infected with a virus is to:
isolate the infected server(s) from the network.
B. identify all potential damage caused by the infection.
C. ensure that the virus database files are current.
D. establish security weaknesses in the firewall.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The priority in this event is to minimize the effect of the virus infection and to prevent it from spreading by removing the infected server(s) from the network. After the network is secured from further infection, the damage assessment can be performed, the virus database updated and any weaknesses sought.

QUESTION 394
Which of the following provides the BKST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

A. The recovery time objective (RTO) was not exceeded during testing
B. Objective testing of the business continuity/disaster recovery plan has been carried out consistently
C. The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
D. Information assets have been valued and assigned to owners per the business continuity plan, disaster recovery plan

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Consistent achievement of recovery time objective (RTO) objectives during testing provides the most objective evidence that business continuity/disaster recovery plan objectives have been achieved. The successful testing of the business continuity/disaster recover) plan within the stated RTO objectives is the most indicative evidence that the business needs are being met. Objective testing of the business continuity/ disaster recovery plan will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning. Mere valuation and assignment of information assets to owners (per the business continuity/disaster recovery plan) will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning.

A.

QUESTION 395

Which of the following situations would be the MOST concern to a security manager?

Audit logs are not enabled on a production server

B. The logon ID for a terminated systems analyst still exists on the system

C. The help desk has received numerous results of users receiving phishing e-mails

D. A Trojan was found to be installed on a system administrator's laptop

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The discovery of a Trojan installed on a system's administrator's laptop is highly significant since this may mean that privileged user accounts and passwords may have been compromised. The other choices, although important, do not pose as immediate or as critical a threat.

QUESTION 396

A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the incident.

B. notify senior management.

C. start containment.

D. notify law enforcement.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Asserting that the condition is a true security incident is the necessary first step in determining the correct response. The containment stage would follow. Notifying senior management and law enforcement could be part of the incident response process that takes place after confirming an incident.

QUESTION 397

When collecting evidence for forensic analysis, it is important to:

A.

A. ensure the assignment of qualified personnel.
B. request the IT department do an image copy.
C. disconnect from the network and isolate the affected devices.

D. ensure law enforcement personnel are present before the forensic analysis commences.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Without the initial assignment of forensic expertise, the required levels of evidence may not be preserved. In choice B. the IT department is unlikely to have that level of expertise and should, thus, be prevented from taking action. Choice C may be a subsequent necessity that comes after choice A. Choice D, notifying law enforcement, will likely occur after the forensic analysis has been completed.

QUESTION 398
What is the BEST method for mitigating against network denial of service (DoS) attacks?

A. Ensure all servers are up-to-date on OS patches
B. Employ packet filtering to drop suspect packets
C. Implement network address translation to make internal addresses nonroutable
D. Implement load balancing for Internet facing devices

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Packet filtering techniques are the only ones which reduce network congestion caused by a network denial of service (DoS) attack. Patching servers, in general, will not affect network traffic. Implementing network address translation and load balancing would not be as effective in mitigating most network DoS attacks.

QUESTION 399
To justify the establishment of an incident management team, an information security manager would find which of the following to be the MOST effective?

A. Assessment of business impact of past incidents
B. Need of an independent review of incident causes
C. Need for constant improvement on the security level
D. Possible business benefits from incident impact reduction

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Business benefits from incident impact reduction would be the most important goal for establishing an incident management team. The assessment of business impact of past incidents would need to be completed to articulate the benefits. Having an independent review benefits the incident management process. The need for constant improvement on the security level is a benefit to the organization.

QUESTION 400
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts
B. Write access violations
C. Concurrent logons
D. Firewall logs

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Since the password for the shared administrative account was obtained through guessing, it is probable that there were multiple unsuccessful logon attempts before the correct password was deduced. Searching the logs for invalid logon attempts could, therefore, lead to the discovery of this unauthorized activity. Because the account is shared, reviewing the logs for concurrent logons would not reveal unauthorized activity since concurrent usage is common in this situation. Write access violations would not necessarily be observed since the information was merely copied and not altered. Firewall logs would not necessarily contain information regarding logon attempts