CISM.530q

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
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

A. Representation by regional business leaders
B. Composition of the board
C. Cultures of the different countries
D. IT security skills

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Culture has a significant impact on how information security will be implemented. Representation by regional business leaders may not have a major influence unless it concerns cultural issues. Composition of the board may not have a significant impact compared to cultural issues. IT security skills are not as key or high impact in designing a multinational information security program as would be cultural issues.

QUESTION 2

Which of the following is the BEST justification to convince management to invest in an information security program?

A. Cost reduction
B. Compliance with company policies
C. Protection of business assets
D. Increased business value

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Investing in an information security program should increase business value and confidence. Cost reduction by itself is rarely the motivator for implementing an information security program. Compliance is secondary to business value. Increasing business value may include protection of business assets.

QUESTION 3
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

A. a statement regarding what the company will do with the information it collects.
B. a disclaimer regarding the accuracy of information on its web site.
C. technical information regarding how information is protected.
D. a statement regarding where the information is being hosted.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Most privacy laws and regulations require disclosure on how information will be used. A disclaimer is not necessary since it does not refer to data privacy. Technical details regarding how information is protected are not mandatory to publish on the web site and in fact would not be desirable. It is not mandatory to say where information is being hosted.

QUESTION 4
The MOST important factor in ensuring the success of an information security program is effective:

A. communication of information security requirements to all users in the organization.
B. formulation of policies and procedures for information security.
C. alignment with organizational goals and objectives.
D. monitoring compliance with information security policies and procedures.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The success of security programs is dependent upon alignment with organizational goals and objectives. Communication is a secondary step. Effective communication and education of users is a critical determinant of success but alignment with organizational goals and objectives is the most important factor for success. Mere formulation of policies without effective communication to users will not ensure success. Monitoring compliance with information security policies and procedures can be, at best, a detective mechanism that will not lead to success in the midst of uninformed users.

QUESTION 5
Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

A. Key control monitoring
B. A robust security awareness program
C. A security program that enables business activities
D. An effective security architecture

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A security program enabling business activities would be most helpful to achieve alignment between information security and organization objectives. All of the other choices are part of the security program and would not individually and directly help as much as the security program.

QUESTION 6
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

A. Continuous analysis, monitoring and feedback
B. Continuous monitoring of the return on security investment (ROSD
C. Continuous risk reduction
D. Key risk indicator (KRD setup to security management processes

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
To improve the governance framework and achieve a higher level of maturity, an organization needs to conduct continuous analysis, monitoring and feedback compared to the current state of maturity. Return on security investment (ROSD may show the performance result of the security-related activities; however, the result is interpreted in terms of money and extends to multiple facets of security initiatives. Thus, it may not be an adequate option. Continuous risk reduction would demonstrate the effectiveness of the security governance framework, but does not indicate a higher level of maturity. Key risk indicator (KRD setup is a tool to be used in internal control assessment. KRI setup presents a threshold to alert management when controls are being compromised in business processes. This is a control tool rather than a maturity model support tool.

QUESTION 7
The MOST complete business case for security solutions is one that.

A. includes appropriate justification.
B. explains the current risk profile.
C. details regulatory requirements.
D. identifies incidents and losses.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

QUESTION 8
Which of the following is MOST important to understand when developing a meaningful information security strategy?

A. Regulatory environment
B. International security standards
C. Organizational risks
D. Organizational goals

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Alignment of security with business objectives requires an understanding of what an organization is trying to accomplish. The other choices are all elements that must be considered, but their importance is secondary and will vary depending on organizational goals.

QUESTION 9
Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness.
B. It is easier to manage and control.
C. It is more responsive to business unit needs.
D. It provides a faster turnaround for security requests.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization. Decentralization allows you to use field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

QUESTION 10
Which of the following would help to change an organization's security culture?

A. Develop procedures to enforce the information security policy

B. Obtain strong management support
C. Implement strict technical security controls
D. Periodically audit compliance with the information security policy

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

QUESTION 11
The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

A. return on investment (ROD.
B. a vulnerability assessment.
C. annual loss expectancy (ALE).
D. a business case.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A business case shows both direct and indirect benefits, along with the investment required and the expected returns, thus making it useful to present to senior management. Return on investment (ROD would only provide the costs needed to preclude specific risks, and would not provide other indirect benefits such as process improvement and learning. A vulnerability assessment is more technical in nature and would only identify and assess the vulnerabilities. This would also not provide insights on indirect benefits. Annual loss expectancy (ALE) would not weigh the advantages of implementing single sign-on (SSO) in comparison to the cost of implementation.

QUESTION 12
The FIRST step in establishing a security governance program is to:

A. conduct a risk assessment.
B. conduct a workshop for all end users.
C. prepare a security budget.
D. obtain high-level sponsorship.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The establishment of a security governance program is possible only with the support and sponsorship of top management since security governance projects are enterprise wide and integrated into business processes. Conducting a risk assessment, conducting a workshop for all end users and preparing a security budget all follow once high-level sponsorship is obtained.

QUESTION 13
An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees Hood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

A. conflicting security controls with organizational needs.
B. strong protection of information resources.
C. implementing appropriate controls to reduce risk.
D. proving information security's protective abilities.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The needs of the organization were not taken into account, so there is a conflict. This example is not strong protection; it is poorly configured. Implementing appropriate controls to reduce risk is not an appropriate control as it is being used. This does not prove the ability to protect, but proves the ability to interfere with business.

QUESTION 14
An organization's information security strategy should be based on:

A. managing risk relative to business objectives.
B. managing risk to a zero level and minimizing insurance premiums.
C. avoiding occurrence of risks so that insurance is not required.
D. transferring most risks to insurers and saving on control costs.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Organizations must manage risks to a level that is acceptable for their business model, goals and objectives. A zero-level approach may be costly and not provide the effective benefit of additional revenue to the organization. Long-term maintenance of this approach may not be cost effective. Risks vary as business models, geography, and regulatory- and operational processes change. Insurance covers only a small portion of risks and requires that the organization have certain operational controls in place.

QUESTION 15
Which of the following should be included in an annual information security budget that is submitted for management approval?

A. A cost-benefit analysis of budgeted resources
B. All of the resources that are recommended by the business
C. Total cost of ownership (TCO)
D. Baseline comparisons

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A brief explanation of the benefit of expenditures in the budget helps to convey the context of how the purchases that are being requested meet goals and objectives, which in turn helps build credibility for the information security function or program. Explanations of benefits also help engage senior management in the support of the information security program. While the budget should consider all inputs and recommendations that are received from the business, the budget that is ultimately submitted to management for approval should include only those elements that are intended for purchase. TCO may be requested by management and may be provided in an addendum to a given purchase request, but is not usually included in an annual budget. Baseline comparisons (cost

comparisons with other companies or industries) may be useful in developing a budget or providing justification in an internal review for an individual purchase, but would not be included with a request for budget approval.

QUESTION 16
Which of the following is a benefit of information security governance?

A. Reduction of the potential for civil or legal liability
B. Questioning trust in vendor relationships
C. Increasing the risk of decisions based on incomplete management information
D. Direct involvement of senior management in developing control processes

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:
Information security governance decreases the risk of civil or legal liability. The remaining answers are incorrect. Option D appears to be correct, but senior management would provide oversight and approval as opposed to direct involvement in developing control processes.

QUESTION 17
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 18
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 19
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 20

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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
Which of the following is the **MOST** important reason for an organization to develop an information security governance program?

A. Establishment of accountability
B. Compliance with audit requirements
C. Monitoring of security incidents
D. Creation of tactical solutions

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 32
The **PRIMARY** purpose of aligning information security with corporate governance objectives is to:

A. build capabilities to improve security processes.
B. consistently manage significant areas of risk.
C. identify an organization's tolerance for risk.
D. re-align roles and responsibilities.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is the **MOST** important consideration for designing an effective information security governance framework?

A. Defined metrics
B. Continuous audit cycle
C. Security policy provisions
D. Security controls automation

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 34
The **PRIMARY** goal of information security governance to an organization is to:

A. align with business processes
B. align with business objectives
C. establish a security strategy
D. manage security costs

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 35

Which of the following is the **BEST** way to integrate information security into corporate governance?

A. Engage external security consultants in security initiatives.
B. Conduct comprehensive information security management training for key stakeholders.
C. Ensure information security processes are part of the existing management processes.
D. Require periodic security risk assessments be performed.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 36
Which of the following is the **MOST** effective way of ensuring that business units comply with an information security governance framework?

A. Integrating security requirements with processes
B. Performing security assessments and gap analysis
C. Conducting a business impact analysis (BIA)
D. Conducting information security awareness training

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
QUESTION 37
Which of the following **BEST** demonstrates alignment between information security governance and corporate governance?

A. Average number of security incidents across business units
B. Security project justifications provided in terms of business value
C. Number of vulnerabilities identified for high-risk information assets
D. Mean time to resolution for enterprise-wide security incidents

Correct Answer: B

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 38
The **MOST** important element in achieving executive commitment to an information security governance program is:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 39
After implementing an information security governance framework, which of the following would provide the **BEST** information to develop an information security project plan?

A. Risk heat map
B. Recent audit results
C. Balanced scorecard
D. Gap analysis

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 40

An information security manager's **PRIMARY** objective for presenting key risks to the board of directors is to:

A. meet information security compliance requirements.
B. ensure appropriate information security governance.
C. quantity reputational risks.
D. re-evaluate the risk appetite.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is **MOST** helpful in integrating information security governance with corporate governance?

A. Assigning the implementation of information security governance to the steering committee.
B. Including information security processes within operational and management processes.
C. Providing independent reports of information security efficiency and effectiveness to the board.
D. Aligning the information security governance to a globally accepted framework.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
QUESTION 42
Which of the following is the **BEST** way to align security and business strategies?

A. Include security risk as part of corporate risk management.
B. Develop a balanced scorecard for security.
C. Establish key performance indicators (KPIs) for business through security processes.
D. Integrate information security governance into corporate governance.

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 43
When developing an information security governance framework, which of the following should be the **FIRST** activity?

A. Integrate security within the system's development life-cycle process.
B. Align the information security program with the organization's other risk and control activities.
C. Develop policies and procedures to support the framework.
D. Develop response measures to detect and ensure the closure of security breaches.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 44
Which of the following is the **MOST** effective way for senior management to support the integration of information security governance into corporate governance?

A. Develop the information security strategy based on the enterprise strategy.
B. Appoint a business manager as heard of information security.
C. Promote organization-wide information security awareness campaigns.
D. Establish a steering committee with representation from across the organization.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 45
Which of the following would **BEST** help to ensure the alignment between information security and business functions?

A. Developing information security polices
B. Establishing an information security governance committee
C. Establishing a security awareness program
D. Providing funding for information security efforts

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 46
When establishing an information security governance framework, it is **MOST** important for an information security manager to understand:

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

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is a **PRIMARY** responsibility of the information security governance function?
A. Defining security strategies to support organizational programs
B. Ensuring adequate support for solutions using emerging technologies
C. Fostering a risk-aware culture to strengthen the information security program
D. Advising senior management on optimal levels of risk appetite and tolerance

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is the **MOST** important requirement for the successful implementation of security governance?

A. Implementing a security balanced scorecard
B. Performing an enterprise-wide risk assessment
C. Mapping to organizational strategies
D. Aligning to an international security framework

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 49
A large organization is in the process of developing its information security program that involves working with several complex organizational functions. Which of the following will **BEST** enable the successful implementation of this program?

A. Security governance
B. Security policy
C. Security metrics
D. Security guidelines

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a **PRIMARY** responsibility of an information security governance committee?

A. Analyzing information security policy compliance reviews

B. Approving the purchase of information security technologies
C. Reviewing the information security strategy
D. Approving the information security awareness training strategy

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 51
An information security manager discovers that the organization's new information security policy is not being followed across all departments. Which of the following should be of **GREATEST** concern to the information security manager?

A. Different communication methods may be required for each business unit.
B. Business unit management has not emphasized the importance of the new policy.
C. The corresponding controls are viewed as prohibitive to business operations.
D. The wording of the policy is not tailored to the audience.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 52
An organization has detected potential risk emerging from noncompliance with new regulations in its industry.
Which of the following is the **MOST** important reason to report this situation to senior management?

A. The risk profile needs to be updated.
B. An external review of the risk needs to be conducted.
C. Specific monitoring controls need to be implemented.
D. A benchmark analysis needs to be performed.

Correct Answer: B

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 53
Which of the following is the **BEST** way for information security manager to identify compliance with information security policies within an organization?

A. Analyze system logs.
B. Conduct security awareness testing.
C. Perform vulnerability assessments.
D. Conduct periodic audits.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 54
Quantitative risk analysis is MOST appropriate when assessment data:

A. include customer perceptions.
B. contain percentage estimates.C. do not contain specific details.
D. contain subjective information.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

QUESTION 55
Which of the following is the MOST appropriate use of gap analysis?

A. Evaluating a business impact analysis (BIA)
B. Developing a balanced business scorecard
C. Demonstrating the relationship between controls
D. Measuring current state vs. desired future state

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a business impact analysis (BIA), developing a balanced business scorecard or demonstrating the relationship between variables.

QUESTION 56
Identification and prioritization of business risk enables project managers to:

A. establish implementation milestones.
B. reduce the overall amount of slack time.
C. address areas with most significance.
D. accelerate completion of critical paths.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:
Explanation:

Identification and prioritization of risk allows project managers to focus more attention on areas of greater importance and impact. It will not reduce the overall amount of slack time, facilitate establishing implementation milestones or allow a critical path to be completed any sooner.

QUESTION 57
A risk analysis should:

A. include a benchmark of similar companies in its scope.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.

D. give more weight to the likelihood vs. the size of the loss.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A risk analysis should take into account the potential size and likelihood of a loss. It could include comparisons with a group of companies of similar size. It should not assume an equal degree of protection for all assets since assets may have different risk factors. The likelihood of the loss should not receive greater emphasis than the size of the loss; a risk analysis should always address both equally.

QUESTION 58
The recovery point objective (RPO) requires which of the following?

A. Disaster declaration
B. Before-image restoration
C. System restoration
D. After-image processing

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

QUESTION 59
Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

A. Systems operation procedures are not enforced
B. Change management procedures are poor
C. Systems development is outsourced

D. Systems capacity management is not performed

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed by third-party vendors are becoming commonplace and do not represent an increase in security risk as much as poor change management. Poor capacity management may not necessarily represent a security risk.

QUESTION 60
Which of the following BEST describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

QUESTION 61
The decision as to whether a risk has been reduced to an acceptable level should be determined by:

A. organizational requirements.
B. information systems requirements.
C. information security requirements.
D. international standards.

Correct Answer: A

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Organizational requirements should determine when a risk has been reduced to an acceptable level. Information systems and information security should not make the ultimate determination. Since each organization is unique, international standards of best practice do not represent the best solution.

QUESTION 62
Which of the following is the PRIMARY reason for implementing a risk management program?

A. Allows the organization to eliminate risk
B. Is a necessary part of management's due diligence
C. Satisfies audit and regulatory requirements
D. Assists in incrementing the return on investment (ROD

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The key reason for performing risk management is that it is part of management's due diligence. The elimination of all risk is not possible. Satisfying audit and regulatory requirements is of secondary importance. A risk management program may or may not increase the return on investment (ROD.

QUESTION 63
Which of the following groups would be in the BEST position to perform a risk analysis for a business?
A. External auditors
B. A peer group within a similar businessC. Process owners
D. A specialized management consultant

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties do not have that level of detailed knowledge on the inner workings of the business. Management consultants are expected to have the necessary skills in risk analysis techniques but are still less effective than a group with intimate knowledge of the business.

QUESTION 64
A successful risk management program should lead to:

A. optimization of risk reduction efforts against cost.
B. containment of losses to an annual budgeted amount.
C. identification and removal of all man-made threats.
D. elimination or transference of all organizational risks.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Successful risk management should lead to a breakeven point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, while losses cannot be budgeted in advance with absolute certainty.

QUESTION 65
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

A. Customer data stolen
B. An electrical power outage
C. A web site defaced by hackers
D. Loss of the software development team

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The effect of the theft of customer data or web site defacement by hackers could lead to a permanent decline in customer confidence, which does not lend itself to measurement by quantitative techniques. Loss of a majority of the software development team could have similar unpredictable repercussions. However, the loss of electrical power for a short duration is more easily measurable and can be quantified into monetary amounts that can be assessed with quantitative techniques.

QUESTION 66
The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

A. hourly billing rate charged by the carrier.
B. value of the data transmitted over the network.
C. aggregate compensation of all affected business users.
D. financial losses incurred by affected business units.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

QUESTION 67
Which of the following is the MOST usable deliverable of an information security risk analysis?

A. Business impact analysis (BIA) report
B. List of action items to mitigate risk
C. Assignment of risks to process owners
D. Quantification of organizational risk

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Although all of these are important, the list of action items is used to reduce or transfer the current level of risk. The other options materially contribute to the way the actions are implemented.

QUESTION 68
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

A. Tree diagrams
B. Venn diagrams
C. Heat charts
D. Bar charts

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Meat charts, sometimes referred to as stoplight charts, quickly and clearly show the current status of remediation efforts. Venn diagrams show the connection between sets; tree diagrams are useful for decision analysis; and bar charts show relative size.

QUESTION 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
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 78
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 79
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 80
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 81
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.

A.

QUESTION 82

The PRIMARY objective of a risk management program is to:

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 83

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,

A.
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 84
When performing an information risk analysis, an information security manager should FIRST:

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 85
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.

A.
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 86

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 87
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 88
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 89
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 90
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 91
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 92
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 93
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 94
Which of the following would a security manager establish to determine the target for restoration of normal processing?

A. Recover time objective (RTO)
C.

D.

B. Maximum tolerable outage (MTO)
Recovery point objectives (RPOs)
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 95
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 96

C.

D.
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
User testing
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 97
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.

C.

D.

QUESTION 98

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.
the cost of countermeasure outweighs the value of the asset and potential loss.
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 99

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:

C.

D.
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 100
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 resultsCustomer personal information

C.

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 101
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 102
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 103
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 104
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 105
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 106
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 107
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 108
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
B. Create a strong random password
C. Ask for a vendor patch
D. 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 109
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 110
Which of the following would BEST address the risk of data leakage?

A. File backup procedures
B. Database integrity checks
C. Acceptable use policies
D. 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 111
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.

QUESTION 112
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 113
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 114
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 115
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 116
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 117
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 118
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 119
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 120
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 121
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 122
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 123
Previously accepted risk should be:

A. re-assessed periodically since the risk can be escalated to an unacceptable level due to revised conditions.
B. accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptable.
C. avoided next time since risk avoidance provides the best protection to the company.
D. removed from the risk log once it is accepted.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Acceptance of risk should be regularly reviewed to ensure that the rationale for the initial risk acceptance is still valid within the current business context. The rationale for initial risk acceptance may no longer be valid due to change(s) and. hence, risk cannot be accepted permanently. Risk is an inherent part of business and it is impractical and costly to eliminate all risk. Even risks that have been accepted should be monitored for changing conditions that could alter the original decision.

QUESTION 124
An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

A. perform a comprehensive assessment of the organization's exposure to the hacker's techniques.
B. initiate awareness training to counter social engineering.
C. immediately advise senior management of the elevated risk.

D. increase monitoring activities to provide early detection of intrusion.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information about possible significant new risks from credible sources should be provided to management along with advice on steps that need to be taken to counter the threat. The security manager should assess the risk, but senior management should be immediately advised. It may be prudent to initiate an awareness campaign subsequent to sounding the alarm if awareness training is not current. Monitoring activities should also be increased.

QUESTION 125
Which of the following steps should be performed FIRST in the risk assessment process?

A. Staff interviews

B. Threat identification
C. Asset identification and valuation
D. Determination of the likelihood of identified risks

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk. Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

QUESTION 126
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism

C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A challenge/response mechanism prevents replay attacks by sending a different random challenge in each authentication event. The response is linked to that challenge. Therefore, capturing the authentication handshake and replaying it through the network will not work. Using hashes by itself will not prevent a replay. A WEP key will not prevent sniffing (it just takes a few more minutes to break the WEP key if the attacker does not already have it) and therefore will not be able to prevent recording and replaying an authentication handshake. HTTP Basic Authentication is clear text and has no mechanisms to prevent replay.

QUESTION 127
An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

A. Nothing, since a risk assessment was completed during development.
B. A vulnerability assessment should be conducted.
C. A new risk assessment should be performed.
D. The new vendor's SAS 70 type II report should be reviewed.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The risk assessment process is continual and any changes to an established process should include a new- risk assessment. While a review of the SAS 70 report and a vulnerability assessment may be components of a risk assessment, neither would constitute sufficient due diligence on its own.

QUESTION 128
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 129
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 130
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 131
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 132
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 133
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 134
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 135
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 136
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 137
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 138
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 139
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 140
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 141
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 142
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 143
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 144
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 145
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 146

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 147
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 148
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 149
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 150
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 151
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 152
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 153
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 154
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 155
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 156
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 157
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 158
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 159
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 160
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 161

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 162
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 163
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 164
Which of the following is the **PRIMARY** goal of a risk management program?

A. Implement preventive controls against threats.
B. Manage the business impact of inherent risks.
C. Manage compliance with organizational policies.
D. Reduce the organization's risk appetite.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 165
A risk management program will be **MOST** effective when:

A. risk appetite is sustained for a long period
B. risk assessments are repeated periodically
C. risk assessments are conducted by a third party
D. business units are involved in risk assessments

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 166

The objective of risk management is to reduce risk to the minimum level that is:

A. compliant with security policies
B. practical given industry and regulatory environments. C. achievable from technical and financial perspectives.
D. acceptable given the preference of the organization.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 167
The **MOST** important objective of monitoring key risk indicators (KRIs) related to information security is to:
A. identify change in security exposures.
B. reduce risk management costs.
C. meet regulatory compliance requirements.
D. minimize the loss from security incidents.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 168
Which of the following would be **MOST** helpful in determining an organization’s current capacity to mitigate risk?

A. Capability maturity model

B. Business impact analysis
C. IT security risk and exposure
D. Vulnerability assessment

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 169
Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager's most important action is to:

A. provide senior management with risk treatment options.
B. design and implement controls to reduce the risk.
C. consult external third parties on how to treat the risk.
D. ensure that employees are aware of the risk.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 170
An organization's marketing department wants to use an online collaboration service which is not in compliance with the information security policy. A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

A. the information security manager
B. business senior management
C. the chief risk officer
D. the compliance officer.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 171
The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the **GREATEST** when:

A. standard operating procedures are not formalized
B. the IT infrastructure is diverse
C. IDS sensors are misconfigured.
D. operations and monitoring are handled by different teams.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 172
An information security manager has been informed of a new vulnerability in an online banking application, and patch to resolve this issue is expected to be released in the next 72 hours. The information security manager's **MOST** important course of action should be to:

A. assess the risk and advise senior management.
B. identify and implement mitigating controls.
C. run the application system in offline mode.
D. perform a business impact analysis (BIA).

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 173
An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done **NEXT** to address this concern?

A. Conduct a risk analysis
B. Escalate to the chief risk officer
C. Conduct a vulnerability analysis
D. Determine compensating controls

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 174
In risk assessment, after the identification of threats to organizational assets, the information security manager would:

A. evaluate the controls currently in place.

B. implement controls to achieve target risk levels.
C. request funding for the security program.
D. determine threats to be reported to upper management.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 175
During a security assessment, an information security manager finds a number of security patches were not installed on a server hosting a critical business application. The application owner did not approve the patch installation to avoid interrupting the application.

Which of the following should be the information security manager's **FIRST** course of action?

A. Escalate the risk to senior management.
B. Communicate the potential impact to the application owner.
C. Report the risk to the information security steering committee.
D. Determine mitigation options with IT management.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 176
Risk identification, analysis, and mitigation activities can BEST be integrated into business life cycle processes by linking them to:

A. compliance testing
B. configuration management
C. continuity planning
D. change management

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 177
Which of the following is the **PRIMARY** reason for performing an analysis of the threat landscape on a regular basis?

A. To determine the basis for proposing an increase in security budgets.
B. To determine if existing business continuity plans are adequate.

C. To determine if existing vulnerabilities present a risk.
D. To determine critical information for executive management.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 178
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 179
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 180
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. 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.

QUESTION 181
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 182
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 183
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 184
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 185
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 186
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 187
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 188
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 189

A.
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?

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 190
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.

A.

QUESTION 191

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

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 192

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

A.
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 193
Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

A. Intrusion detection system (IDS)
B. IP address packet filtering
C. Two-factor authentication
D. Embedded digital signature

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Two-factor authentication provides an additional security mechanism over and above that provided by passwords alone. This is frequently used by mobile users needing to establish connectivity to a corporate network. IP address packet filtering would protect against spoofing an internal address but would not provide strong authentication. An intrusion detection system (IDS) can be used to detect an external attack but would not help in authenticating a user attempting to connect. Digital signatures ensure that transmitted information can be attributed to the named sender.

QUESTION 194
What is an appropriate frequency for updating operating system (OS) patches on production servers?

A. During scheduled rollouts of new applications
B. According to a fixed security patch management schedule
C. Concurrently with quarterly hardware maintenance
D. Whenever important security patches are released

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Patches should be applied whenever important security updates are released. They should not be delayed to coincide with other scheduled rollouts or maintenance. Due to the possibility of creating a system outage, they should not be deployed during critical periods of application activity such as month-end or quarter-end closing.

QUESTION 195
Which of the following devices should be placed within a DMZ?

A. Proxy server
B. Application server
C. Departmental server
D. Data warehouse server

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An application server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Data warehouse and departmental 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. A proxy server forms the inner boundary of the DMZ but is not placed within it.

QUESTION 196
A border router should be placed on which of the following?

A. Web server
B. IDS server
C. Screened subnet
D. Domain boundary

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

QUESTION 197
An e-commerce order fulfillment web server should generally be placed on which of the following?

A. Internal network

B. Demilitarized zone (DMZ)
C. Database server
D. Domain controller

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An e-commerce order fulfillment web server should be placed within a DMZ to protect it and the internal network from external attack. Placing it on the internal network would expose the internal network to potential attack from the Internet. Since a database server should reside on the internal network, the same exposure would exist. Domain controllers would not normally share the same physical device as a web server.

QUESTION 198
Secure customer use of an e-commerce application can BEST be accomplished through:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Encryption would be the preferred method of ensuring confidentiality in customer communications with an e-commerce application. Strong passwords, by themselves, would not be sufficient since the data could still be intercepted, while two-factor authentication would be impractical. Digital signatures would not provide a secure means of communication. In most business-to-customer (B-to-C) web applications, a digital signature is also not a practical solution.

QUESTION 199
What is the BEST defense against a Structured Query Language (SQL) injection attack?

A. Regularly updated signature files

B. A properly configured firewall
C. An intrusion detection system
D. Strict controls on input fields

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Structured Query Language (SQL) injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent of fooling the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written; software is available to test for such weaknesses. All other choices would fail to prevent such an attack.

QUESTION 200
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

If an intrusion detection system (IDS) is not properly tuned it will generate an unacceptable number of false positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to operating system hardening, while encryption and packet filtering would not be as relevant.

QUESTION 201
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

A. Authentication

B. Hardening
C. Encryption
D. Nonrepudiation

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Cardholder data should be encrypted using strong encryption techniques. Hardening would be secondary in importance, while nonrepudiation would not be as relevant. Authentication of the point-of-sale (POS) terminal is a previous step to acquiring the card information.

QUESTION 202
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager
B. Establish predetermined automatic expiration dates
C. Require managers to e-mail security when the user leaves
D. Ensure each individual has signed a security acknowledgement

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Predetermined expiration dates are the most effective means of removing systems access for temporary users. Reliance on managers to promptly send in termination notices cannot always be counted on, while requiring each individual to sign a security acknowledgement would have little effect in this case.

QUESTION 203
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. corporate internal auditor.
B. System developers/analysts.
C. key business process owners.

D. corporate legal counsel.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Business process owners are in the best position to understand how new regulatory requirements may affect their systems. Legal counsel and infrastructure management, as well as internal auditors, would not be in as good a position to fully understand all ramifications.

QUESTION 204
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

A. Ease of installation
B. Product documentation
C. Available support
D. System overhead

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Monitoring products can impose a significant impact ON system overhead for servers and networks. Product documentation, telephone support and ease of installation, while all important, would be secondary.

QUESTION 205
Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

A. Never use open source tools
B. Focus only on production servers
C. Follow a linear process for attacks
D. Do not interrupt production processes

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments since, if compromised, the test environment could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than a linear process.

QUESTION 206
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

A. Stress testing
B. Patch management
C. Change management
D. Security baselines

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

QUESTION 207
The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

A. helps ensure that communications are secure.
B. increases security between multi-tier systems.
C. allows passwords to be changed less frequently.
D. eliminates the need for secondary authentication.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:
Virtual Private Network (VPN) tunneling for remote users provides an encrypted link that helps ensure secure communications. It does not affect password change frequency, nor does it eliminate the need for secondary authentication or affect security within the internal network.

QUESTION 208
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

A. Boundary router
B. Strong encryption
C. Internet-facing firewall
D. Intrusion detection system (IDS)

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Strong encryption is the most effective means of protecting wireless networks. Boundary routers, intrusion detection systems (IDSs) and firewalling the Internet would not be as effective.

QUESTION 209
Which of the following is MOST effective in protecting against the attack technique known as phishing?

A. Firewall blocking rules
B. Up-to-date signature files
C. Security awareness training
D. Intrusion detection monitoring

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Phishing relies on social engineering techniques. Providing good security awareness training will best reduce the likelihood of such an attack being successful. Firewall rules, signature files and intrusion detection system (IDS) monitoring will be largely unsuccessful at blocking this kind of attack.

QUESTION 210
When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

A. The firewall should block all inbound traffic during the outage
B. All systems should block new logins until the problem is corrected
C. Access control should fall back to no synchronized mode
D. System logs should record all user activity for later analysis

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The best mechanism is for the system to fallback to the original process of logging on individually to each system. Blocking traffic and new logins would be overly restrictive to the conduct of business, while recording all user activity would add little value.

QUESTION 211
Which of the following is the MOST important risk associated with middleware in a client-server environment?

A. Server patching may be prevented
B. System backups may be incomplete
C. System integrity may be affected
D. End-user sessions may be hijacked

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely to occur.

QUESTION 212
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?
A. Security in storage and transmission of sensitive data B.
Provider's level of compliance with industry standards
C. Security technologies in place at the facility
D. Results of the latest independent security review

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Mow the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

QUESTION 213
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

A. Configuration of firewalls
B. Strength of encryption algorithms
C. Authentication within application
D. Safeguards over keys

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

If keys are in the wrong hands, documents will be able to be read regardless of where they are on the network. Choice A is incorrect because firewalls can be perfectly configured, but if the keys make it to the other side, they will not prevent the document from being decrypted. Choice B is incorrect because even easy encryption algorithms require adequate resources to break, whereas encryption keys can be easily used. Choice C is incorrect because the application "front door" controls may be bypassed by accessing data directly.

QUESTION 214
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

A. Encryption
B. Digital certificate
C. Digital signature
D. I lashing algorithm

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

To preserve confidentiality of a message while in transit, encryption should be implemented. Choices B and C only help authenticate the sender and the receiver. Choice D ensures integrity.

QUESTION 215
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 216
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 217
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 218
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 219
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 220
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 221
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 222
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 223
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 224
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 225

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 226
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?

A. Regular review of access control lists
B. Security guard escort of visitors
C. 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 227
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 228
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
C. 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 229

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.

QUESTION 230
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 231

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 232
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 233

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

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 234
During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have BEST help to prevent this occurrence?

A. Validation of senior management's risk tolerance
B. Updates to the business impact analysis (BIA)
C. More effective disaster recovery plan (DRP) testing
D. Improvements to incident identification methods

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 235
The implementation of a capacity plan would prevent:

A. file system overload arising from distributed denial-of-service attacks
B. system downtime for scheduled security maintenance
C. software failures arising from exploitation of buffer capacity vulnerabilities
D. application failures arising from insufficient hardware resources

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 236
Which of the following defines the triggers within a business continuity plan (BCP)?

A. Disaster recovery plan
B. Needs of the organization
C. Gap analysis
D. Information security policy

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 237
An organization plans to allow employees to use their own devices on the organization's network. Which of the following is the information security manager's BEST course of action?

A. Implement automated software
B. Assess associated risk
C. Conduct awareness training
D. Update the security policy

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 238
When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

A. give the business a measure of the organization's overall readiness
B. provide participants with situations to ensure understanding of their roles
C. measure management engagement as part of an incident response team
D. challenge the incident response team to solve the problem under pressure

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanations
Tabletop scenarios that need to be completed with one hour per scenario using full escalation as per decision trees to accurately simulate and evaluate responses of each team member and the processes within the playbooks.

QUESTION 239
Which of the following is the PRIMARY advantage of desk checking a business continuity plan (BCP)?

A. Assesses the availability and compatibility a backup hardware
B. Allows for greater participation be management and the IT department
C. Ensures that appropriate follow-up work is performed on noted issues
D. Provides a low-cost method of assessing the BCP's completeness

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 240
An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

A. Results from a gap analysis
B. Results from a business impact analysis

C. Deadlines and penalties for noncompliance
D. An inventory of security controls currently in place

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 241
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:

Correct Answer:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 242
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 243
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 244
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.
Establish business unit security working groups.
D

QUESTION 245
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 246
Which of the following should be of **MOST** concern to an information security manager reviewing an organization's data classification program?

A. The program allows exceptions to be granted.
B. Labeling is not consistent throughout the organization.
C. Data retention requirement are not defined.
D. The classifications do not follow industry best practices.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

D.

Correct Answer:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 247
Which of the following would the **BEST** demonstrate the added value of an information security program?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 248
An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personally identifiable information (PII).

Which of the following would be **MOST** helpful for this purpose?

A. Metrics related to program effectiveness
B. Written policies and standards
C. Privacy awareness training
D. Risk assessments of privacy-related applications

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 249
Which of the following should be **PRIMARILY** included in a security training program for business process owners?

A. Impact of security risks
B. Application vulnerabilities
C. Application recovery time
List of security incidents reported
A

QUESTION 250
A CIO has asked the organization's information security manager to provide both one-year and five-year plans for the information security program. What is the **PRIMARY** purpose for the long-term plan?

A. To create formal requirements to meet projected security needs for the future
B. To create and document a consistent progression of security capabilities
C. To prioritize risks on a longer scale than the one-year plan
D. To facilitate the continuous improvement of the IT organization

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 251
Which of the following has the **MOST** direct impact on the usability of an organization's asset classification program?

A. The granularity of classifications in the hierarchy
B. The frequency of updates to the organization's risk register
C. The business objectives of the organization
D. The support of senior management for the classification scheme
D.

Correct Answer:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

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

Explanation/Reference:
QUESTION 252
Which of the following is the MOST important factor to ensure information security is meeting the organization's objectives?

A. Internal audit's involvement in the security process
B. Implementation of a control self-assessment process
C. Establishment of acceptable risk thresholds
D. Implementation of a security awareness program

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 253
An organization has an approved bring your own device (BYOD) program. Which of the following is the **MOST** effective method to enforce application control on personal devices?

A. Establish a mobile device acceptable use policy.
B. Implement a mobile device management solution.
C. Educate users regarding the use of approved applications.
D. Implement a web application firewall.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 254
Which of the following is the **MOST** important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

A. The ability to remotely locate devices
B. The ability to centrally manage devices
C. The ability to restrict unapproved applications
The ability to classify types of devices
B

QUESTION 255
Which of the following is the **GREATEST** benefit of integrating information security program requirements into vendor management?

A. The ability to reduce risk in the supply chain
B. The ability to meet industry compliance requirements
C. The ability to define service level agreements (SLAs)
D. The ability to improve vendor performance

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 256
Which of the following is a step in establishing a security policy?

A. Developing platform-level security baselines
B. Creating a RACI matrix
C. Implementing a process for developing and maintaining the policy
D. Developing configuration parameters for the network

Correct Answer: C
D.

Correct Answer:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 257
The **BEST** time to ensure that a corporation acquires secure software products when outsourcing software development is during:

A. corporate security reviews.
B. contract performance audits.
C. contract negotiation.
D. security policy development.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 258
Which of the following is the **BEST** way to determine if an organization's current risk is within the risk appetite?

A. Conducting a business impact analysis (BIA)
B. Implementing key performance indicators (KPIs)
C. Implementing key risk indicators (KRIs)
D. Developing additional mitigating controls

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 259
An organization with a strict need-to-know information access policy is about to launch a knowledge management intranet.

Which of the following is the **MOST** important activity to ensure compliance with existing security policies?

A. Develop a control procedure to check content before it is published.
B. Change organization policy to allow wider use of the new web site.
C. Ensure that access to the web site is limited to senior managers and the board.
Password-protect documents that contain confidential information.
D

QUESTION 260
Which of the following if the MOST significant advantage of developing a well-defined information security strategy?

A. Support for buy-in from organizational employees
B. Allocation of resources to highest priorities
C. Prevention of deviations from risk tolerance thresholds
D. Increased maturity of incident response processes

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 261
Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?

A. The indicator should possess a high correlation with a specific risk and be measured on a regular basis.
B. The indicator should focus on IT and accurately represent risk variances.
C. The indicator should align with key performance indicators and measure root causes of process performance issues.
D. The indicator should provide a retrospective view of risk impacts and be measured annually.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation
D.

Correct Answer:
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation/Reference:

QUESTION 262

When implementing security architecture, an information security manager **MUST** ensure that security controls:

A. form multiple barriers against threats.
B. are transparent.
C. are the least expensive.
D. are communicated through security policies.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 263
An information security manager is reviewing the business case for a security project that is entering the development phase. It is determined that the estimated cost of the controls is now greater than the risk being mitigated.

The information security manager's **BEST** recommendation would be to:

A. eliminate some of the controls from the project scope.
B. discontinue the project to release funds for other efforts.
C. pursue the project until the benefits cover the costs.
D. slow the pace of the project to spread costs over a longer period.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 264
The chief information security officer (CISO) has developed an information security strategy, but is struggling to obtain senior management commitment for funds to implement the strategy.

Which of the following is the **MOST** likely reason?

A. The strategy does not include a cost-benefit analysis.
B. The CISO reports to the CIO.
C. There was a lack of engagement with the business during development.
D. The strategy does not comply with security standards.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 265
An organization wants to enable digital forensics for a business-critical application. Which of the following will **BEST** help to support this objective?

A. Install biometric access control.
B. Develop an incident response plan.
C. Define data retention criteria.
D. Enable activity logging.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 266
An organization is developing a disaster recovery plan for a data center that hosts multiple applications. The application recovery sequence would **BEST** be determined through an analysis of:

A. Key performance indicators (KPIs)
B. Recovery time objectives (RTOs)
C. Recovery point objectives (RPOs)
D. The data classification scheme

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:

QUESTION 267
Which of the following should be the **PRIMARY** goal of an information security manager when designing information security policies?

A. Reducing organizational security risk
B. Improving the protection of information
C. Minimizing the cost of security controls
D. Achieving organizational objectives

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 268
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus **PRIMARILY** on defining:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 269
When developing security processes for handling credit card data on the business unit's information system, the information security manager should **FIRST**:

A. review corporate policies regarding credit card information.
B. implement the credit card companies' security requirements.
C. ensure that systems handle credit card data are segmented.
D. review industry's best practices for handling secure payments.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 270
When developing a disaster recovery plan, which of the following would be **MOST** helpful in prioritizing the order in which systems should be recovered?

A. Performing a business impact analysis
B. Measuring the volume of data in each system
C. Reviewing the information security policy
D. Reviewing the business strategy

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 271
When developing an information security strategy, the **MOST** important requirement is that:

A. standards capture the intent of management.
B. a schedule is developed to achieve objectives.
C. the desired outcome is known.
D. critical success factors (CSFs) are developed.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 272

Which of the following is the **PRIMARY** responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 273

Which of the following should be the **PRIMARY** consideration when selecting a recovery site?

A. Regulatory requirements
B. Recovery time objective
C. Geographical location
D. Recovery point objective

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 274

Management has announced the acquisition of a new company. The information security manager of parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies.

To **BEST** address this concern, the information security manager should: A.

escalate concern for conflicting access rights to management.

B. implement consistent access control standards.
C. review access rights as the acquisition integration occurs.
D. perform a risk assessment of the access rights.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 275
Which of the following would be **MOST** helpful to the information security manager tasked with enforcing enhanced password standards?

A. Conducting password strength testing
B. Reeducating end users on creating strong complex passwords
C. Implementing a centralized identity management system
D. Implementing technical password controls to include strong complexity

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 276
Which of the following is the **MOST** practical control that an organization can implement to prevent unauthorized downloading of data to universal serial bus (USB) storage devices?

A. Two-factor authentication
B. Restrict drive usage
C. Strong encryption

D. Disciplinary action

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

QUESTION 277
Which of the following is the **BEST** method to determine whether an information security program meets an organization's business objectives?

A. Implement performance measures.
B. Review against international security standards.
C. Perform a business impact analysis (BIA).
D. Conduct an annual enterprise-wide security evaluation.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 278
What is the **BEST** course of action when an information security manager finds an external service provider has not implemented adequate controls for safeguarding the organization's critical data?

A. Assess the impact of the control gap.
B. Initiate contract renegotiations.
C. Purchase additional insurance.
D. Conduct a controls audit of the provider.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:

QUESTION 279

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

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 280
Which of the following should be the **PRIMARY** consideration for an information security manager when designing security controls for a newly acquired business application?

A. Known vulnerabilities in the application
B. The IT security architecture framework
C. Cost-benefit analysis of current controls
D. Business processes supported by the application

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 281
Which of the following would provide the **BEST** justification for a new information security investment?

A. Results of a comprehensive threat analysis.
B. Projected reduction in risk.
C. Senior management involvement in project prioritization.
D. Defined key performance indicators (KPIs)

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 282
Which of the following is the **PRIMARY** reason for executive management to be involved in establishing an enterprise's security management framework?

A. To determine the desired state of enterprise security
B. To establish the minimum level of controls needed
C. To satisfy auditors' recommendations for enterprise security
D. To ensure industry best practices for enterprise security are followed

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 283
The **PRIMARY** reason for establishing a data classification scheme is to identify:

A. data ownership.
B. data-retention strategy.
C. appropriate controls.
D. recovery priorities.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 284
Which of the following needs to be established between an IT service provider and its clients to the **BEST** enable adequate continuity of service in preparation for an outage?

A. Data retention policies
B. Server maintenance plans
C. Recovery time objectives

D. Reciprocal site agreement

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 285
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 286
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 287
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 288
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 289
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 290

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 291
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 292
What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodic review of network configuration

B. Review intrusion detection system (IDS) logs for evidence of attacks
C. Periodically perform penetration tests
D. Daily review of server logs for evidence of hacker activity

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:
Explanation:

Due to the complexity of firewall rules and router tables, plus the sheer size of intrusion detection systems (IDSs) and server logs, a physical review will be insufficient. The best approach for confirming the adequacy of these configuration settings is to periodically perform attack and penetration tests.

QUESTION 293
Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Reduced number of security violation reports
B. A quantitative evaluation to ensure user comprehension
C. Increased interest in focus groups on security issues
D. Increased number of security violation reports

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

To truly judge the effectiveness of security awareness training, some means of measurable testing is necessary to confirm user comprehension. Focus groups may or may not provide meaningful feedback but, in and of themselves, do not provide metrics. An increase or reduction in the number of violation reports may not be indicative of a high level of security awareness.

QUESTION 294
Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used
B. Provide clear directions to IT staff
C. Monitor intrusion detection system (IDS) and firewall logs closely

D. Establish clear rules of engagement

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
It is critical to establish a clear understanding on what is permissible during the engagement. Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used. As for monitoring the intrusion detection system (IDS) and firewall, and providing directions to IT staff, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

QUESTION 295
Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

A. Restrict the available drive allocation on all PCs
B. Disable universal serial bus (USB) ports on all desktop devices
C. Conduct frequent awareness training with noncompliance penalties
D. Establish strict access controls to sensitive information

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Restricting the ability of a PC to allocate new drive letters ensures that universal serial bus (USB) drives or even CD-writers cannot be attached as they would not be recognized by the operating system. Disabling USB ports on all machines is not practical since mice and other peripherals depend on these connections. Awareness training and sanctions do not prevent copying of information nor do access controls.

QUESTION 296
Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

A. Signal strength
B. Number of administrators
C. Bandwidth
D. Encryption strength

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
The number of individuals with access to the network configuration presents a security risk. Encryption strength is an area where wireless networks tend to fall short; however, the potential to compromise the entire network is higher when an inappropriate number of people can alter the configuration. Signal strength and network bandwidth are secondary issues.

QUESTION 297
Good information security standards should:

A. define precise and unambiguous allowable limits.
B. describe the process for communicating violations.
C. address high-level objectives of the organization.
D. be updated frequently as new software is released.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

A security standard should clearly state what is allowable; it should not change frequently. The process for communicating violations would be addressed by a security procedure, not a standard. High-level objectives of an organization would normally be addressed in a security policy.

QUESTION 298
Good information security procedures should:

A. define the allowable limits of behavior.
B. underline the importance of security governance.
C. describe security baselines for each platform.
D. be updated frequently as new software is released.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Security procedures often have to change frequently to keep up with changes in software. Since a procedure is a how-to document, it must be kept up-to-date with frequent changes in software. A security standard such as platform baselines — defines behavioral limits, not the how-to process; it should not change frequently. High-level objectives of an organization, such as security governance, would normally be addressed in a security policy.

QUESTION 299

What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

A. all use weak encryption.
B. are decrypted by the firewall.
C. may be quarantined by mail filters.
D. may be corrupted by the receiving mail server.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Often, mail filters will quarantine zip files that are password-protected since the filter (or the firewall) is unable to determine if the file contains malicious code. Many zip file products are capable of using strong encryption. Such files are not normally corrupted by the sending mail server.

QUESTION 300

A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

A. Sign a legal agreement assigning them all liability for any breach
B. Remove all trading partner access until the situation improves
C. Set up firewall rules restricting network traffic from that location
D. Send periodic reminders advising them of their noncompliance

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

It is incumbent on an information security manager to see to the protection of their organization's network, but to do so in a manner that does not adversely affect the conduct of business. This can be accomplished by adding specific traffic restrictions for that particular location. Removing all access will likely result in lost business. Agreements and reminders do not protect the integrity of the network.

QUESTION 301
Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

A. define the circumstances where cryptography should be used.
B. define cryptographic algorithms and key lengths.
C. describe handling procedures of cryptographic keys.
D. establish the use of cryptographic solutions.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

There should be documented standards-procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

QUESTION 302
Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

A. The number of false positives increases
B. The number of false negatives increases
C. Active probing is missed
D. Attack profiles are ignored

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Failure to tune an intrusion detection system (IDS) will result in many false positives, especially when the threshold is set to a low value. The other options are less likely given the fact that the threshold for sounding an alarm is set to a low value.

QUESTION 303
What is the MOST appropriate change management procedure for the handling of emergency program changes?

A. Formal documentation does not need to be completed before the change
B. Business management approval must be obtained prior to the change
C. Documentation is completed with approval soon after the change
D. All changes must follow the same process

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Even in the case of an emergency change, all change management procedure steps should be completed as in the case of normal changes. The difference lies in the timing of certain events. With an emergency change, it is permissible to obtain certain approvals and other documentation on "the morning after" once the emergency has been satisfactorily resolved. Obtaining business approval prior to the change is ideal but not always possible.

QUESTION 304
Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

A. Information security officer
B. Security steering committee
C. Data owner
D. Data custodian

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Routine administration of all aspects of security is delegated, but senior management must retain overall responsibility. The information security officer supports and implements information security for senior management. The data owner is responsible for categorizing data security requirements. The data custodian supports and implements information security as directed.

QUESTION 305

The PRIMARY focus of the change control process is to ensure that changes are:

A.
authorized. B.
applied.
C. documented.
D. tested.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

All steps in the change control process must be signed off on to ensure proper authorization. It is important that changes are applied, documented and tested; however, they are not the primary focus.

QUESTION 306
An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

A. Research best practices
B. Meet with stakeholders
C. Establish change control procedures
D. Identify critical systems

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

No new process will be successful unless it is adhered to by all stakeholders; to the extent stakeholders have input, they can be expected to follow the process. Without consensus agreement from the stakeholders, the scope of the research is too wide; input on the current environment is necessary to focus research effectively. It is premature to implement procedures without stakeholder consensus and research. Without knowing what the process will be the parameters to baseline are unknown as well.

QUESTION 307
A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?
Enable access through a separate device that requires adequate authentication

A.
B. Implement manual procedures that require password change after each use
C. Request the vendor to add multiple user IDs
D. Analyze the logs to detect unauthorized access

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual. Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but. because it is detective, it would not be the most effective in this instance.

QUESTION 308
Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

A. User security procedures
B. Business process flow
C. IT security policy
D. Regulatory requirements

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

IT management should ensure that mechanisms are implemented in line with IT security policy. Procedures are determined by the policy. A user security procedure does not describe the access control mechanism in place. The business process flow is not relevant to the access control mechanism. The organization's own policy and procedures should take into account regulatory requirements.

QUESTION 309
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

A. The right to conduct independent security reviews
B. A legally binding data protection agreement
C. Encryption between the organization and the provider
D. A joint risk assessment of the system

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A key requirement of an outsource contract involving critical business systems is the establishment of the organization's right to conduct independent security reviews of the provider's security controls. A legally binding data protection agreement is also critical, but secondary to choice A, which permits examination of the actual security controls prevailing over the system and. as such, is the more effective risk management tool. Network encryption of the link between the organization and the provider may well be a requirement, but is not as critical since it would also be included in choice A. A joint risk assessment of the system in conjunction with the outsource provider may be a compromise solution, should the right to conduct independent security reviews of the controls related to the system prove contractually difficult.

QUESTION 310
Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

A. Card key door locks
B. Photo identification
C. Awareness training
D. Biometric scanners

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. Choices A, B and D are physical controls that, by themselves, would not be effective against tailgating.

A.

QUESTION 311

In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

A. ensure access to individual functions can be granted to individual users only.
B. implement role-based access control in the application.
C. enforce manual procedures ensuring separation of conflicting duties.
D. create service accounts that can only be used by authorized team members.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Role-based access control is the best way to implement appropriate segregation of duties. Roles will have to be defined once and then the user could be changed from one role to another without redefining the content of the role each time. Access to individual functions will not ensure appropriate segregation of duties. Giving a user access to all functions and implementing, in parallel, a manual procedure ensuring segregation of duties is not an effective method, and would be difficult to enforce and monitor. Creating service accounts that can be used by authorized team members would not provide any help unless their roles are properly segregated.

QUESTION 312
In business-critical applications, user access should be approved by the:

A. information security manager.
B. data owner.
C. data custodian.
D. business management.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

A data owner is in the best position to validate access rights to users due to their deep understanding of business requirements and of functional implementation within the application. This responsibility should be enforced by the policy. An information security manager will coordinate and execute the implementation of the role-based access control. A data custodian will ensure that proper safeguards are in place to protect the data from unauthorized access; it is not the data custodian's responsibility to assign access rights. Business management is not. in all cases, the owner of the data.

QUESTION 313
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 314
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 315
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

A. Review the procedures for granting access
B. Establish procedures for granting emergency access
C. Meet with data owners to understand business needs
D. Redefine and implement proper access rights

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

An information security manager must understand the business needs that motivated the change prior to taking any unilateral action. Following this, all other choices could be correct depending on the priorities set by the business unit.

QUESTION 316
When security policies are strictly enforced, the initial impact is that:

A. they may have to be modified more frequently.
B. they will be less subject to challenge.
C. the total cost of security is increased.
D. the need for compliance reviews is decreased.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

When security policies are strictly enforced, more resources are initially required, thereby increasing, the total cost of security. There would be less need for frequent modification. Challenges would be rare and the need for compliance reviews would not necessarily be less.

QUESTION 317
A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

A. an effective control over connectivity and continuity.
B. a service level agreement (SLA) including code escrow.
C. a business impact analysis (BIA).

D. a third-party certification.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The principal risk focus is the connection procedures to maintain continuity in case of any contingency. Although an information security manager may be interested in the service level agreement (SLA), code escrow is not a concern. A business impact analysis (BIA) refers to contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

QUESTION 318
Which of the following should be in place before a black box penetration test begins?

A. IT management approval
B. Proper communication and awareness training
C. A clearly stated definition of scope
D. An incident response plan

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Having a clearly stated definition of scope is most important to ensure a proper understanding of risk as well as success criteria, IT management approval may not be required based on senior management decisions. Communication, awareness and an incident response plan are not a necessary requirement. In fact, a penetration test could help promote the creation and execution of the incident response plan.

QUESTION 319
What is the MOST important element to include when developing user security awareness material?

A. Information regarding social engineering
B. Detailed security policies
C. Senior management endorsement

D. Easy-to-read and compelling information

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Making security awareness material easy and compelling to read is the most important success factor. Users must be able to understand, in easy terms, complex security concepts in a way that makes compliance more accessible. Choice A would also be important but it needs to be presented in an adequate format. Detailed security policies might not necessarily be included in the training materials. Senior management endorsement is important for the security program as a whole and not necessarily for the awareness training material.

QUESTION 320
What is the MOST important success factor in launching a corporate information security awareness program?

A. Adequate budgetary support
B. Centralized program management
C. Top-down approach
D. Experience of the awareness trainers

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Senior management support will provide enough resources and will focus attention to the program: training should start at the top levels to gain support and sponsorship. Funding is not a primary concern. Centralized management does not provide sufficient support. Trainer experience, while important, is not the primary success factor.

QUESTION 321
Which of the following events generally has the highest information security impact?

A. Opening a new office
B. Merging with another organization
C. Relocating the data center

D. Rewiring the network

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Merging with or acquiring another organization causes a major impact on an information security management function because new vulnerabilities and risks are inherited. Opening a new office, moving the data center to a new site, or rewiring a network may have information security risks, but generally comply with corporate security policy and are easier to secure.

QUESTION 322
The configuration management plan should PRIMARILY be based upon input from:

A. business process owners.
B. the information security manager.
C. the security steering committee.
D. IT senior management.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Although business process owners, an information security manager and the security steering committee may provide input regarding a configuration management plan, its final approval is the primary responsibility of IT senior management.

QUESTION 323
Which of the following is the MOST effective, positive method to promote security awareness?

A. Competitions and rewards for compliance
B. Lock-out after three incorrect password attempts
C. Strict enforcement of password formats
D. Disciplinary action for noncompliance

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

QUESTION 324
An information security program should focus on:

A. best practices also in place at peer companies.
B. solutions codified in international standards.
C. key controls identified in risk assessments.
D. continued process improvement.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Risk assessment identifies the appropriate controls to mitigate identified business risks that the program should implement to protect the business. Peer industry best practices, international standards and continued process improvement can be used to support the program, but these cannot be blindly implemented without the consideration of business risk.

QUESTION 325
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

A. Database administrator (DBA)
B. Finance department management
C. Information security manager
D. IT department management

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

QUESTION 326
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 327
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 328
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 329
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 330
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 331
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 332
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 333
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 334
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 335
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 336
Which of the following is the MOST likely outcome of a well-designed information security awareness course?

A. Increased reporting of security incidents to the incident response function
B. Decreased reporting of security incidents to the incident response function
C. Decrease in the number of password resets
D. Increase in the number of identified system vulnerabilities

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

A well-organized information security awareness course informs all employees of existing security policies, the importance of following safe practices for data security anil the need to report any possible security incidents to the appropriate individuals in the organization. The other choices would not be the likely outcomes.

QUESTION 337
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

A. Review of various security models
B. Discussion of how to construct strong passwords
C. Review of roles that have privileged access
D. Discussion of vulnerability assessment results

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 338
A critical component of a continuous improvement program for information security is:
A. measuring processes and providing feedback.
B. developing a service level agreement (SLA) for security.
C. tying corporate security standards to a recognized international standard.
D. ensuring regulatory compliance.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

If an organization is unable to take measurements that will improve the level of its safety program. then continuous improvement is not possible. Although desirable, developing a service level agreement (SLA) for security, tying corporate security standards to a recognized international standard and ensuring regulatory compliance are not critical components for a continuous improvement program.

QUESTION 339
The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager

A. report risks in other departments.
B. obtain support from other departments.
C. report significant security risks.
D. have knowledge of security standards.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The IT manager needs to report the security risks in the environment pursuant to the security review, including risks in the IT implementation. Choices A, B and D are important, but not the main responsibilities or job requirements.

QUESTION 340

An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

A. Rule-based
B. Mandatory
C. Discretionary
D. Role-based

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Role-based access control is effective and efficient in large user communities because it controls system access by the roles defined for groups of users. Users are assigned to the various roles and the system controls the access based on those roles. Rule-based access control needs to define the access rules, which is troublesome and error prone in large organizations. In mandatory access control, the individual's access to information resources needs to be defined, which is troublesome in large organizations. In discretionary access control, users have access to resources based on predefined sets of principles, which is an inherently insecure approach.

QUESTION 341
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

A. an audit of the service provider uncovers no significant weakness.
B. the contract includes a nondisclosure agreement (NDA) to protect the organization's intellectual property.
C. the contract should mandate that the service provider will comply with security policies.
D. the third-party service provider conducts regular penetration testing.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is critical to include the security requirements in the contract based ON the company's security policy to ensure that the necessary security controls are implemented by the service provider. The audit is normally a one-time effort and cannot provide ongoing assurance of the security. A nondisclosure agreement

(NDA) should be part of the contract; however, it is not critical to the security of the web site. Penetration testing alone would not provide total security to the web site; there are lots of controls that cannot be tested through penetration testing.

QUESTION 342
Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

A. To mitigate technical risks
B. To have an independent certification of network security
C. To receive an independent view of security exposures
D. To identify a complete list of vulnerabilities

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Even though the organization may have the capability to perform penetration testing with internal resources, third-party penetration testing should be performed to gain an independent view of the security exposure. Mitigating technical risks is not a direct result of a penetration test. A penetration test would not provide certification of network security nor provide a complete list of vulnerabilities.

QUESTION 343
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

A. Prepare an impact assessment report.
B. Conduct a penetration test.
C. Obtain approval from senior management.
D. Back up the firewall configuration and policy files.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

An impact assessment report needs to be prepared first by providing the justification for the change, analysis of the changes to be made, the impact if the change does not work as expected, priority of the change and urgency of the change request. Choices B. C and D could be important steps, but the impact assessment report should be performed before the other steps.

QUESTION 344
An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

A. Request that the third-party provider perform background checks on their employees.
B. Perform an internal risk assessment to determine needed controls.
C. Audit the third-party provider to evaluate their security controls.
D. Perform a security assessment to detect security vulnerabilities.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

An internal risk assessment should be performed to identify the risk and determine needed controls. A background check should be a standard requirement for the service provider. Audit objectives should be determined from the risk assessment results. Security assessment does not cover the operational risks.

QUESTION 345
Which of the following would raise security awareness among an organization's employees?

A. Distributing industry statistics about security incidents
B. Monitoring the magnitude of incidents
C. Encouraging employees to behave in a more conscious manner
D. Continually reinforcing the security policy

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Employees must be continually made aware of the policy and expectations of their behavior. Choice A would have little relevant bearing on the employee's behavior. Choice B does not involve the employees. Choice C could be an aspect of continual reinforcement of the security policy.

QUESTION 346
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

A. Attempt to reset several passwords to weaker values

B. Install code to capture passwords for periodic audit
C. Sample a subset of users and request their passwords for review
D. Review general security settings on each platform

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Reviewing general security settings on each platform will be the most efficient method for determining password strength while not compromising the integrity of the passwords. Attempting to reset several passwords to weaker values may not highlight certain weaknesses. Installing code to capture passwords for periodic audit, and sampling a subset of users and requesting their passwords for review, would compromise the integrity of the passwords.

QUESTION 347
What is the MOST cost-effective method of identifying new vendor vulnerabilities?

A. External vulnerability reporting sources
B. Periodic vulnerability assessments performed by consultants
C. Intrusion prevention software
D. honey pots located in the DMZ

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

External vulnerability sources are going to be the most cost-effective method of identifying these vulnerabilities. The cost involved in choices B and C would be much higher, especially if performed at regular intervals. Honeypots would not identify all vendor vulnerabilities. In addition, honeypots located in the DMZ can create a security risk if the production network is not well protected from traffic from compromised honey pots.

QUESTION 348
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audits.

B. Perform periodic penetration testing.
C. Define and monitor security metrics.
D. Survey business units for feedback.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Defining and monitoring security metrics is a good approach to analyze the performance of the security management process since it determines the baseline and evaluates the performance against the baseline to identify an opportunity for improvement. This is a systematic and structured approach to process improvement. Audits will identify deficiencies in established controls; however, they are not effective in evaluating the overall performance for improvement. Penetration testing will only uncover technical vulnerabilities, and cannot provide a holistic picture of information security management, feedback is subjective and not necessarily reflective of true performance.

QUESTION 349
An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

A. validate and sanitize client side inputs.
B. harden the database listener component.
C. normalize the database schema to the third normal form.
D. ensure that the security patches are updated on operating systems.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

SQL injection vulnerability arises when crafted or malformed user inputs are substituted directly in SQL queries, resulting into information leakage. Hardening the database listener does enhance the security of the database; however, it is unrelated to the SQL injection vulnerability. Normalization is related to the effectiveness and efficiency of the database but not to SQL injection vulnerability. SQL injections may also be observed in normalized databases. SQL injection vulnerability exploits the SQL query design, not the operating system.

QUESTION 350
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

A. uses multiple redirects for completing a data commit transaction.
B. has implemented cookies as the sole authentication mechanism.
C. has been installed with a non-legitimate license key.
D. is hosted on a server along with other applications.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

XSRF exploits inadequate authentication mechanisms in web applications that rely only on elements such as cookies when performing a transaction. XSRF is related to an authentication mechanism, not to redirection. Option C is related to intellectual property rights, not to XSRF vulnerability. Merely hosting multiple applications on the same server is not the root cause of this vulnerability.

QUESTION 351
Of the following, retention of business records should be PRIMARILY based on:

A. periodic vulnerability assessment.
B. regulatory and legal requirements.
C. device storage capacity and longevity.
D. past litigation.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Retention of business records is a business requirement that must consider regulatory and legal requirements based on geographic location and industry. Options A and C are important elements for making the decision, but the primary driver is the legal and regulatory requirements that need to be followed by all companies. Record retention may take into consideration past litigation, but it should not be the primary decision factor.

QUESTION 352
An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

A. A due diligence security review of the business partner's security controls

B. Ensuring that the business partner has an effective business continuity program
C. Ensuring that the third party is contractually obligated to all relevant security requirements
D. Talking to other clients of the business partner to check references for performance

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

The key requirement is that the information security manager ensures that the third party is contractually bound to follow the appropriate security requirements for the process being outsourced. This protects both organizations. All other steps are contributory to the contractual agreement, but are not key.

QUESTION 353
An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

A. Right to audit
B. Nondisclosure agreement
C. Proper firewall implementation
D. Dedicated security manager for monitoring compliance

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

QUESTION 354
Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

A. Provide security awareness training to the third-party provider's employees
B. Conduct regular security reviews of the third-party provider
C. Include security requirements in the service contract

D. Request that the third-party provider comply with the organization's information security policy

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Regular security audits and reviews of the practices of the provider to prevent potential information security damage will help verify the security of outsourced services. Depending on the type of services outsourced, security awareness may not be necessary. Security requirements should be included in the contract, but what is most important is verifying that the requirements are met by the provider. It is not necessary to require the provider to fully comply with the policy if only some of the policy is related and applicable.

QUESTION 355
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

A. Design a training program for the staff involved to heighten information security awareness B. Set role-based access permissions on the shared folder
C. The end user develops a PC macro program to compare sender and recipient file contents
D. Shared folder operators sign an agreement to pledge not to commit fraudulent activities

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Ideally, requesting that the IT department develop an automated integrity check would be desirable, but given the temporary nature of the problem, the risk can be mitigated by setting stringent access permissions on the shared folder. Operations staff should only have write access and disbursement staff should only have read access, and everyone else, including the administrator, should be disallowed. An information security awareness program and/or signing an agreement to not engage in fraudulent activities may help deter attempts made by employees: however, as long as employees see a chance of personal gain when internal control is loose, they may embark on unlawful activities such as alteration of payment files. A PC macro would be an inexpensive automated solution to develop with control reports. However, sound independence or segregation of duties cannot be expected in the reconciliation process since it is run by an end-user group. Therefore, this option may not provide sufficient proof.

QUESTION 356
Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

A. A problem management process
B. Background screening
C. A change control process
D. Business impact analysis (BIA)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A change control process is the methodology that ensures that anything that could be impacted by a development change will be reevaluated. Problem management is the general process intended to manage all problems, not those specifically related to security. Background screening is the process to evaluate employee references when they are hired. BIA is the methodology used to evaluate risks in the business continuity process.

QUESTION 357
Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

A. Vulnerability scans
B. Penetration tests
C. Code reviews
D. Security audits

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A penetration test is normally the only security assessment that can link vulnerabilities together by exploiting them sequentially. This gives a good measurement and prioritization of risks. Other security assessments such as vulnerability scans, code reviews and security audits can help give an extensive and thorough risk and vulnerability overview', but will not be able to test or demonstrate the final consequence of having several vulnerabilities linked together. Penetration testing can give risk a new perspective and prioritize based on the end result of a sequence of security problems.

QUESTION 358
In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

A. Procedural design
B. Architectural design
C. System design specifications
D. Software development

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

The system design specifications phase is when security specifications are identified. The procedural design converts structural components into a procedural description of the software. The architectural design is the phase that identifies the overall system design, hut not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.

QUESTION 359
Which of the following is generally considered a fundamental component of an information security program?

A. Role-based access control systems
B. Automated access provisioning
C. Security awareness training
D. Intrusion prevention systems (IPSs)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

Without security awareness training, many components of the security program may not be effectively implemented. The other options may or may not be necessary, but are discretionary.

QUESTION 360
How would an organization know if its new information security program is accomplishing its goals?

A. Key metrics indicate a reduction in incident impacts.
B. Senior management has approved the program and is supportive of it.
C. Employees are receptive to changes that were implemented.

D. There is an immediate reduction in reported incidents.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Option A is correct since an effective security program will show a trend in impact reduction. Options B and C may well derive from a performing program, but are not as significant as option A. Option D may indicate that it is not successful.

QUESTION 361
A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

A. it simulates the real-life situation of an external security attack.
B. human intervention is not required for this type of test.
C. less time is spent on reconnaissance and information gathering.
D. critical infrastructure information is not revealed to the tester.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Data and information required for penetration are shared with the testers, thus eliminating time that would otherwise have been spent on reconnaissance and gathering of information. Blind (black box) penetration testing is closer to real life than full disclosure (white box) testing. There is no evidence to support that human intervention is not required for this type of test. A full disclosure (white box) methodology requires the knowledge of the subject being tested.

QUESTION 362
Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A. Acceptable use policy
B. Setting low mailbox limitsC. User awareness training
D. Taking disciplinary action
Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

User awareness training would help in reducing the incidents of employees forwarding spam and chain e-mails since users would understand the risks of doing so and the impact on the organization's information system. An acceptable use policy, signed by employees, would legally address the requirements but merely having a policy is not the best measure. Setting low mailbox limits and taking disciplinary action are a reactive approach and may not help in obtaining proper support from employees.

QUESTION 363
Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

A. Passwords stored in encrypted form
B. User awareness
C. Strong passwords that are changed periodically
D. Implementation of lock-out policies

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Implementation of account lock-out policies significantly inhibits brute-force attacks. In cases where this is not possible, strong passwords that are changed periodically would be an appropriate choice. Passwords stored in encrypted form will not defeat an online brute-force attack if the password itself is easily guessed. User awareness would help but is not the best approach of the options given.

QUESTION 364
Which of the following measures is the MOST effective deterrent against disgruntled stall abusing their privileges?

A. Layered defense strategy
B. System audit log monitoring
C. Signed acceptable use policy
D. High-availability systems

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

A layered defense strategy would only prevent those activities that are outside of the user's privileges. A signed acceptable use policy is often an effective deterrent against malicious activities because of the potential for termination of employment and/or legal actions being taken against the individual. System audit log monitoring is after the fact and may not be effective. High-availability systems have high costs and are not always feasible for all devices and components or systems.

QUESTION 365
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

A. the existence of messages is unknown.
B. required key sizes are smaller.
C. traffic cannot be sniffed.
D. reliability of the data is higher in transit.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

The existence of messages is hidden when using steganography. This is the greatest risk. Keys are relevant for encryption and not for steganography. Sniffing of steganographic traffic is also possible. Option D is not relevant.

QUESTION 366
As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A. considered at the discretion of the information owner.
B. approved by the next higher person in the organizational structure.
C. formally managed within the information security framework.
D. reviewed and approved by the security manager.

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference: Explanation:

A formal process for managing exceptions to information security policies and standards should be included as part of the information security framework. The other options may be contributors to the process but do not in themselves constitute a formal process.

QUESTION 367
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 368
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 369
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 370
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 371
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 372
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 373
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 374
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 375
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 376
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 377
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 378
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 379
A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The **GREATEST** weakness under this system architecture is that:

A. users can gain direct access to the application ID and circumvent data controls.
B. when multiple sessions with the same application ID collide, the database locks up.
C. the database becomes unavailable if the password of the application ID expires.
D. an incident involving unauthorized access to data cannot be tied to a specific user.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 380
A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's **FIRST** course of action?

A. Review the current security policy.
B. Inform senior management of the new regulation.
C. Update the security incident management process.
D. Determine impact to the business.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 381

An organization has decided to implement a security information and event management (SIEM) system. It is **MOST** important for the organization to consider:

A. industry best practices.
B. data ownership.
C. log sources.
D. threat assessments.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 382
Which of the following change management procedures is **MOST** likely to cause concern to the information security manager?

A. Fallback processes are tested the weekend before changes are made.
B. The development manager migrates programs into production.
C. A manual rather than an automated process is used to compare program versions.
D. Users are not notified of scheduled system changes.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 383
A multinational organization wants to monitor outbound traffic for data leakage from the use of unapproved cloud services. Which of the following should be the information security manager's **GREATEST** consideration when implementing this control?

A. Security of cloud services
B. Data privacy regulations
C. Resistance from business users
D. Allocation of monitoring resources

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 384
Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed **NEXT**?

A. Develop an implementation strategy.
B. Schedule the target end date for implementation activities.
C. Budget the total cost of implementation activities.
D. Calculate the residual risk for each countermeasure.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 385
Which of the following would **BEST** assist an IS manager in gaining strategic support from executive management?

A. Annual report of security incidents within the organization
B. Research on trends in global information security breaches
C. Rating of the organization's security, based on international standards
D. Risk analysis specific to the organization

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 386
An emergency change was made to an IT system as a result of a failure. Which of the following should be of **GREATEST** concern to the organization's information security manager?

A. The change did not include a proper assessment of risk.

B. Documentation of the change was made after implementation.
C. The information security manager did not review the change prior to implementation.
D. The operations team implemented the change without regression testing.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 387
The **PRIMARY** advantage of single sign-on (SSO) is that it will:

A. support multiple authentication mechanisms.
B. increase the security related applications.
C. strengthen user password.
D. increase efficiency of access management.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 388
Which of the following is the **MOST** important reason for performing vulnerability assessments periodically?

A. Management requires regular reports.
B. The environment changes constantly.
C. Technology risks must be mitigated.
D. The current threat levels are being assessed.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 389
Which of the following architectures for e-business **BEST** ensures high availability?

A. Availability of an adjacent hot site and a standby server with mirrored copies of critical data
B. Intelligent middleware to direct transactions from a downed system to an alternative
C. A single point of entry allowing transactions to be received and processed quickly
D. Automatic failover to the web site of another e-business that meets the user's needs

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 390
A business case for investment in an information security management infrastructure **MUST** include:

A. evidence that the proposed infrastructure is certified.
B. specifics on the security applications needed.
C. data management methods currently in use.
D. impact of noncompliance with applicable standards.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 391
An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the **MOST** important action of the information security manager?

A. Follow the outsourcer's response plan.
B. Alert the appropriate law enforcement authorities.
C. Refer to the organization's response plan.
D. Notify the outsourcer of the privacy breach.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 392
Which of the following threats is prevented by using token-based authentication?

A. Password sniffing attack on the network
B. Denial of service attack over the network
C. Main-in-the middle attack on the client
D. Session eavesdropping attack on the network

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 393
What of the following is **MOST** important to include in an information security policy?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 394
Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

A. Data ownership
B. Data monitoring
C. Data custodian
D. Data encryption

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 395
When outsourcing data to a cloud service provider, which of the following should be the information security manager's **MOST** important consideration?

A. Roles and responsibilities have been defined for the subscriber organization.
B. Cloud servers are located in the same country as the organization.
C. Access authorization includes biometric security verification.
D. Data stored at the cloud service provider is not co-mingled.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 396
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 397
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 398
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 399

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 400
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 401
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 402
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 403
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 404
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 405
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 406
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 407
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 408
Senior management asks the information security manager for justification before approving the acquisition of a new intrusion detection system (IDS). The **BEST** course of action is to provide:

A. documented industry best practices B. a gap analysis against the new IDS controls.
C. a business case.
D. a business impact analysis (BIA).

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 409
Ensuring that activities performed by outsourcing providers comply with information security policies can **BEST** be accomplished through the use of:

A. service level agreements.
B. independent audits.
C. explicit contract language.
D. local regulations.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 410
Which of the following will **BEST** enable an effective information asset classification process?

A. Reviewing the recovery time objective (RTO) requirements of the asset
B. Analyzing audit findings
C. Including security requirements in the classification process
D. Assigning ownership

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 411
Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered the **MOST** significant exposure?

A. Proxy server
B. Mail relay server
C. Application server
D. Database server

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 412
Which of the following should be the **MOST** important criteria when defining data retention policies?

A. Capacity requirements

B. Audit findings
C. Regulatory requirements
D. Industry best practices

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 413
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities **BEST** supports the concept of integrity?

A. Enforcing service level agreements
B. Implementing a data classification schema
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
QUESTION 414
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the **GREATEST** concern to an information security manager if omitted from the contract?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 415
Which of the following is the **BEST** method to protect consumer private information for an online public website?

A. Encrypt consumer's data in transit and at rest.
B. Apply a masking policy to the consumer data.
C. Use secure encrypted transport layer.
D. Apply strong authentication to online accounts.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 416
Failure to include information security requirements within the build/buy decision would **MOST** likely result in the need for:

A. compensating controls in the operational environment.
B. commercial product compliance with corporate standards.
C. more stringent source programming standards.
D. security scanning of operational platforms.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 417
A business impact analysis should be periodically executed **PRIMARILY** to:

A. validate vulnerabilities on environmental changes.
B. analyze the importance of assets.
C. verify the effectiveness of controls.
D. check compliance with regulations.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 418
The **GREATEST** benefit resulting from well-documented information security procedures is that they:

A. ensure that security policies are consistently applied.
B. ensure that critical processes can be followed by temporary staff.
C. facilitate security training of new staff.
D. provide a basis for auditing security practices.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 419
For an organization with a large and complex IT infrastructure, which of the following elements of a disaster recovery hot site service will require the closest monitoring?

A. Employee access
B. Audit rights
C. Systems configurations
D. Number of subscribers

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 420
Reviewing security objectives and ensuring the integration of security across business units is **PRIMARILY** the focus of the:

A. executive management
B. chief information security officer (CISO)
C. board of directors
D. steering committee.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 421
Which of the following metrics is the **BEST** indicator of an abuse of the change management process that could compromise information security?

A. Small number of change request
B. Large percentage decrease in monthly change requests
C. Percentage of changes that include post-approval supplemental add-ons
D. High ratio of lines of code changed to total lines of code

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 422
Which of the following is the **BEST** criterion to use when classifying assets?

A. The market value of the assets
B. Annual loss expectancy (ALE)
C. Value of the assets relative to the organization
D. Recovery time objective (RTO)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 423
Which of the following is the MOST effective method to prevent an SQL injection in an employee portal?

A. Reconfigure the database schema
B. Enforce referential integrity on the database
C. Conduct code reviews
D. Conduct network penetration testing

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 424
Which of the following is **MOST** important when conducting a forensic investigation?
A. Documenting analysis steps
B. Capturing full system images
C. Maintaining a chain of custody
D. Analyzing system memory

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 425
Which of the following would be the information security manager's **BEST** course of action to gain approval for investment in a technical control?

A. Perform a cost-benefit analysis.
B. Conduct a risk assessment.
C. Calculate the exposure factor.
D. Conduct a business impact analysis (BIA).

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 426
Which of the following is the **BEST** indication of information security strategy alignment with the business?

A. Number of business objectives directly supported by information security initiatives.
B. Percentage of corporate budget allocated to information security initiatives.
C. Number of business executives who have attended information security awareness sessions.
D. Percentage of information security incidents resolved within defined service level agreements.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 427
The **GREATEST** benefit of choosing a private cloud over a public cloud would be:

A. server protection.
B. collection of data forensics.
C. online service availability.
D. containment of customer data.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 428
Which of the following is the **MOST** important consideration when selecting members for an information security steering committee?

A. Cross-functional composition
B. Information security expertise

C. Tenure in the organization
D. Business expertise

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 429
Organization A offers e-commerce services and uses secure transport protocol to protect Internet communication. To confirm communication with Organization A, which of the following would be the **BEST** for a client to verify?

A. The certificate of the e-commerce server
B. The browser's indication of SSL use
C. The IP address of the e-commerce server
D. The URL of the e-commerce server

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 430
Meeting which of the following security objectives **BEST** ensures that information is protected against unauthorized modification?

A. Authenticity
B. Availability
C. Confidentiality
D. Integrity

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 431
An information security steering group should:

A. provide general oversight and guidance.
B. develop information security policies.
C. establish information security baselines.
D. oversee the daily operations of the security program.

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

QUESTION 432
Which of the following should be the PRIMARY basis for an information security strategy?

A. The organization's vision and mission.
B. Information security policies.
C. Results of a comprehensive gap analysis.
D. Audit and regulatory requirements.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 433
Which of the following is an example of a vulnerability?

A. Natural disasters
B. Defective software
C. Ransomware
D. Unauthorized users

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 434
What would be an information security manager's **BEST** recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization's critical data? A. Create an addendum to the existing contract.

B. Cancel the outsourcing contract.
C. Transfer the risk to the provider.
D. Initiate an external audit of the provider's data center.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 435
Which of the following is the **MOST** important reason to monitor information risk on a continuous basis?

A. The risk profile can change over time.
B. The effectiveness of controls can be verified.
C. The cost of controls can be minimized.
D. Risk assessment errors can be identified.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 436
Which of the following is **MOST** important to include in monthly information security reports to the broad?

A. Trend analysis of security metrics

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
QUESTION 437
The PRIMARY purpose of vulnerability assessments is to:

A. determine the impact of potential threats.
B. test intrusion detection systems (IDS) and response procedures.
C. provide clear evidence that the system is sufficiently secure.
D. detect deficiencies that could lead to a system compromise.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 438
Which of the following could be detected by a network intrusion detection system (IDS)?

A. Undocumented open ports
B. Unauthorized file change
C. Internally generated attacks
D. Emailed virus attachments

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 439

The recovery point objective (RPO) is required in which of the following?

A. Information security plan
B. Incident response plan
C. Business continuity plan
D. Disaster recovery plan

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 440
Which of the following is **MOST** important for an information security manager to verify before conducting full-functional continuity testing?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 441
Which of the following is **MOST** important for an information security manager to communicate to senior management regarding the security program?

A. Potential risks and exposures
B. Impact analysis results
C. Security architecture changes
D. User roles and responsibilities

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 442
Which of the following is the **BEST** defense against a brute force attack?

A. Discretionary access control
B. Intruder detection lockout
C. Time-of-day restrictions
D. Mandatory access control

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 443
Which of the following would **BEST** help to ensure an organization's security program is aligned with business objectives?

A. Security policies are reviewed and approved by the chief information officer.
B. The security strategy is reviewed and approved by the organization's executive committee.
C. The organization's board of directors includes a dedicated information security specialist.
D. Project managers receive annual information security awareness training.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:

QUESTION 444
Which of the following will **MOST** effectively minimize the chance of inadvertent disclosure of confidential information?

A. Following the principle of least privilege

B. Restricting the use of removable media
C. Applying data classification rules
D. Enforcing penalties for security policy violations

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 445
The business continuity policy should contain which of the following?

A. Emergency call trees
B. Recovery criteria
C. Business impact assessment (BIA)
D. Critical backups inventory

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

QUESTION 446
The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

A. weaknesses in network security.
B. patterns of suspicious access.
C. how an attack was launched on the network.
D. potential attacks on the internal network.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The most important function of an intrusion detection system (IDS) is to identify potential attacks on the network. Identifying how the attack was launched is secondary. It is not designed specifically to identify weaknesses in network security or to identify patterns of suspicious logon attempts.

QUESTION 447
When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

A. Ensuring accessibility should a disaster occur
B. Versioning control as plans are modified
C. Broken hyperlinks to resources stored elsewhere
D. Tracking changes in personnel and plan assets

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

QUESTION 448
Which of the following is the BEST way to verify that all critical production servers are utilizing up-to- date virus signature files?

A. Verify the date that signature files were last pushed out
B. Use a recently identified benign virus to test if it is quarantined
C. Research the most recent signature file and compare to the console
D. Check a sample of servers that the signature files are current

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that it was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

QUESTION 449
Which of the following are the MOST important criteria when selecting virus protection software?

A. Product market share and annualized cost
B. Ability to interface with intrusion detection system (IDS) software and firewalls
C. Alert notifications and impact assessments for new viruses
D. Ease of maintenance and frequency of updates

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

For the software to be effective, it must be easy to maintain and keep current. Market share and annualized cost, links to the intrusion detection system (IDS) and automatic notifications are all secondary in nature.

QUESTION 450
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 451

A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

A. document how the attack occurred.
B. notify law enforcement.
C. take an image copy of the media.
D. close the accounts receivable system.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Taking an image copy of the media is a recommended practice to ensure legal admissibility. All of the other choices are subsequent and may be supplementary.

QUESTION 452
When collecting evidence for forensic analysis, it is important to:

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 453
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 454
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 455
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.

QUESTION 456
Which of the following is an example of a corrective control?

A. Diverting incoming traffic upon responding to the denial of service (DoS) attack
B. Filtering network traffic before entering an internal network from outside
C. Examining inbound network traffic for viruses
D. Logging inbound network traffic

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Diverting incoming traffic corrects the situation and. therefore, is a corrective control. Choice B is a preventive control. Choices C and D are detective controls.

QUESTION 457
To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

A. Database server
B. Domain name server (DNS)
C. Time server
D. Proxy server

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

To accurately reconstruct the course of events, a time reference is needed and that is provided by the time server. The other choices would not assist in the correlation and review of these logs.

QUESTION 458
A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

A. Ensure that all OS patches are up-to-date
B. Block inbound traffic until a suitable solution is found C. Obtain guidance from the firewall manufacturer.3

 D.

Commission a penetration test

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring dial all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

QUESTION 459
An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

A. use the test equipment in the warm site facility to read the tapes.

B. retrieve the tapes from the warm site and test them.
C. have duplicate equipment available at the warm site.
D. inspect the facility and inventory the tapes on a quarterly basis.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

A warm site is not fully equipped with the company's main systems; therefore, the tapes should be tested using the company's production systems. Inspecting the facility and checking the tape inventory does not guarantee that the tapes are usable.

QUESTION 460
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

A. Business impact analysis (BIA)
B. Risk assessment
C. Vulnerability assessment
D. Business process mapping

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

A business impact analysis (BIA) provides results, such as impact from a security incident and required response times. The BIA is the most critical process for deciding which part of the information system/ business process should be given prioritization in case of a security incident. Risk assessment is a very important process for the creation of a business continuity plan. Risk assessment provides information on the likelihood of occurrence of security incidence and assists in the selection of countermeasures. but not in the prioritization. As in choice B, a vulnerability assessment provides information regarding the security weaknesses of the system, supporting the risk analysis process. Business process mapping facilitates the creation of the plan by providing mapping guidance on actions after the decision on critical business processes has been made-translating business prioritization to IT prioritization. Business process mapping does not help in making a decision, but in implementing a decision.

QUESTION 461
In addition to backup data, which of the following is the MOST important to store offsite in the event of a disaster?

A. Copies of critical contracts and service level agreements (SLAs)
B. Copies of the business continuity plan

C. Key software escrow agreements for the purchased systems
D. List of emergency numbers of service providers

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Without a copy of the business continuity plan, recovery efforts would be severely hampered or may not be effective. All other choices would not be as immediately critical as the business continuity plan itself. The business continuity plan would contain a list of the emergency numbers of service providers.

QUESTION 462
An organization has learned of a security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

A. assess the likelihood of incidents from the reported cause.
B. discontinue the use of the vulnerable technology.
C. report to senior management that the organization is not affected.
D. remind staff that no similar security breaches have taken place.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The security manager should first assess the likelihood of a similar incident occurring, based on available information. Discontinuing the use of the vulnerable technology would not necessarily be practical since it would likely be needed to support the business. Reporting to senior management that the organization is not affected due to controls already in place would be premature until the information security manager can first assess the impact of the incident. Until this has been researched, it is not certain that no similar security breaches have taken place.

QUESTION 463
Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?
A. Communicating specially drafted messages by an authorized person
B. Refusing to comment until recovery
C. Referring the media to the authorities
D. Reporting the losses and recovery strategy to the media

Correct Answer: A

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Proper messages need to be sent quickly through a specific identified person so that there are no rumors or statements made that may damage reputation. Choices B, C and D are not recommended until the message to be communicated is made clear and the spokesperson has already spoken to the media.

QUESTION 464
During the security review of organizational servers, it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs.
As a FIRST step, the security manager should:

A. copy sample files as evidence.
B. remove access privileges to the folder containing the data.
C. report this situation to the data owner.
D. train the HR team on properly controlling file permissions.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The data owner should be notified prior to any action being taken. Copying sample files as evidence is not advisable since it breaches confidentiality requirements on the file. Removing access privileges to the folder containing the data should be done by the data owner or by the security manager in consultation with the data owner, however, this would be done only after formally reporting the incident. Training the human resources (MR) team on properly controlling file permissions is the method to prevent such incidents in the future, but should take place once the incident reporting and investigation activities are completed.

QUESTION 465
Which of the following has the highest priority when defining an emergency response plan?
A. Critical data
B. Critical infrastructure
C. Safety of personnel
D. Vital records

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

QUESTION 466
The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

A. enable independent and objective review of the root cause of the incidents.
B. obtain support for enhancing the expertise of the third-party teams.
C. identify lessons learned for further improving the information security management process.
D. obtain better buy-in for the information security program.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

It is always desirable to avoid the conflict of interest involved in having the information security team carries out the post event review. Obtaining support for enhancing the expertise of the third-party teams is one of the advantages, but is not the primary driver. Identifying lessons learned for further improving the information security management process is the general purpose of carrying out the post event review. Obtaining better buy-in for the information security program is not a valid reason for involving third-party teams.

QUESTION 467
The MOST important objective of a post incident review is to: A.

capture lessons learned to improve the process.

B. develop a process for continuous improvement.
C. develop a business case for the security program budget.
D. identify new incident management tools.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The main purpose of a post incident review is to identify areas of improvement in the process. Developing a process for continuous improvement is not true in every case. Developing a business case for the security program budget and identifying new incident management tools may come from the analysis of the incident, but are not the key objectives.

QUESTION 468
Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

A. Incident response metrics
B. Periodic auditing of the incident response process
C. Action recording and review
D. Post incident review

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Post event reviews are designed to identify gaps and shortcomings in the actual incident response process so that these gaps may be improved over time. The other choices will not provide the same level of feedback in improving the process.

QUESTION 469
The FIRST step in an incident response plan is to:

A. notify- the appropriate individuals.
B. contain the effects of the incident to limit damage.
C. develop response strategies for systematic attacks.
D. validate the incident.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Appropriate people need to be notified; however, one must first validate the incident. Containing the effects of the incident would be completed after validating the incident. Developing response strategies for systematic attacks should have already been developed prior to the occurrence of an incident.

QUESTION 470
An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

A. Inform senior management.
B. Determine the extent of the compromise.
C. Report the incident to the authorities.
D. Communicate with the affected customers.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Before reporting to senior management, affected customers or the authorities, the extent of the exposure needs to be assessed.

QUESTION 471
A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

A. Run a port scan on the system
B. Disable the logon ID
C. Investigate the system logs
D. Validate the incident

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

When investigating a possible incident, it should first be validated. Running a port scan on the system, disabling the logon IDs and investigating the system logs may be required based on preliminary forensic investigation, but doing so as a first step may destroy the evidence.

QUESTION 472
The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

A. regulatory' requirements.
B. business requirements.
C. financial value.
D. IT resource availability.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

The criticality to business should always drive the decision. Regulatory requirements could be more flexible than business needs. The financial value of an asset could not correspond to its business value. While a consideration, IT resource availability is not a primary factor.

QUESTION 473
An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

A. Unsure that critical data on the server are backed up.
B. Shut down the compromised server.
C. Initiate the incident response process.
D. Shut down the network.

Correct Answer: C
The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

Explanation:

QUESTION 474
An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

A. Shut down and power off the server.
B. Duplicate the hard disk of the server immediately.
C. Isolate the server from the network.
D. Copy the database log file to a protected server.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Isolating the server will prevent further intrusions and protect evidence of intrusion activities left in memory and on the hard drive. Some intrusion activities left in virtual memory may be lost if the system is shut down. Duplicating the hard disk will only preserve the evidence on the hard disk, not the evidence in virtual memory, and will not prevent further unauthorized access attempts. Copying the database log file to a protected server will not provide sufficient evidence should the organization choose to pursue legal recourse.

QUESTION 475
Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

A. Setting up a backup site
B. Maintaining redundant systems
C. Aligning with recovery time objectives (RTOs)
D. Data backup frequency

Correct Answer: C
BCP, DRP should align with business RTOs. The RTO represents the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RTO must be taken into consideration when prioritizing systems for recovery efforts to ensure that those systems that the business requires first are the ones that are recovered first.

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

Explanation:

QUESTION 476
Of the following, which is the MOST important aspect of forensic investigations?

A. The independence of the investigator
B. Timely intervention
C. Identifying the perpetrator
D. Chain of custody

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Establishing the chain of custody is one of the most important steps in conducting forensic investigations since it preserves the evidence in a manner that is admissible in court. The independence of the investigator may be important, but is not the most important aspect. Timely intervention is important for containing incidents, but not as important for forensic investigation. Identifying the perpetrator is important, but maintaining the chain of custody is more important in order to have the perpetrator convicted in court.

QUESTION 477
In the course of examining a computer system for forensic evidence, data on the suspect media were inadvertently altered. Which of the following should have been the FIRST course of action in the investigative process?

A. Perform a backup of the suspect media to new media.
B. Perform a bit-by-bit image of the original media source onto new media.
C. Make a copy of all files that are relevant to the investigation.
D. Run an error-checking program on all logical drives to ensure that there are no disk errors. **Correct Answer:** B

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

Explanation:

The original hard drive or suspect media should never be used as the source for analysis. The source or original media should be physically secured and only used as the master to create a bit-by-bit image. The original should be stored using the appropriate procedures, depending on location. The image created for forensic analysis should be used. A backup does not preserve 100 percent of the data, such as erased or deleted files and data in slack space — which may be critical to the investigative process. Once data from the source are altered, they may no longer be admissible in court. Continuing the investigation, documenting the date, time and data altered, are actions that may not be admissible in legal proceedings. The organization would need to know the details of collecting and preserving forensic evidence relevant to their jurisdiction.

QUESTION 478
Which of the following recovery strategies has the GREATEST chance of failure?

A. Hot site
B. Redundant site
C. Reciprocal arrangement
D. Cold site

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

A reciprocal arrangement is an agreement that allows two organizations to back up each other during a disaster. This approach sounds desirable, but has the greatest chance of failure due to problems in keeping agreements and plans up to date. A hot site is incorrect because it is a site kept fully equipped with processing capabilities and other services by the vendor. A redundant site is incorrect because it is a site equipped and configured exactly like the primary site. A cold site is incorrect because it is a building having a basic environment such as electrical wiring, air conditioning, flooring, etc. and is ready to receive equipment in order to operate.

QUESTION 479
Recovery point objectives (RPOs) can be used to determine which of the following?

A. Maximum tolerable period of data loss
B. Maximum tolerable downtime
C. Baseline for operational resiliency
D. Time to restore backups

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference: Explanation:

The RPO is determined based on the acceptable data loss in the case of disruption of operations. It indicates the farthest point in time prior to the incident to which it is acceptable to recover the data. RPO effectively quantifies the permissible amount of data loss in the case of interruption. It also dictates the frequency of backups required for a given data set since the smaller the allowable gap in data, the more frequent that backups must occur.

QUESTION 480
Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

A. Preparedness tests
B. Paper tests
C. Full operational tests
D. Actual service disruption

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: Explanation:

Preparedness tests would involve simulation of the entire test in phases and help the team better understand and prepare for the actual test scenario. Options B, C and D are not cost-effective ways to establish plan effectiveness. Paper tests in a walk-through do not include simulation and so there is less learning and it is difficult to obtain evidence that the team has understood the test plan. Option D is not recommended in most cases. Option C would require an approval from management is not easy or practical to test in most scenarios and may itself trigger a disaster.

QUESTION 481
When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

A. Assigning responsibility for acquiring the data
B. Locating the data and preserving the integrity of the data
C. Creating a forensically sound image
D. Issuing a litigation hold to all affected parties

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation
Explanation/Reference:
Explanation:

Locating the data and preserving data integrity is the only correct answer because it represents the primary responsibility of an investigator and is a complete and accurate statement of the first priority. While assigning responsibility for acquiring the data is a step that should be taken, it is not the first step or the highest priority. Creating a forensically sound image may or may not be a necessary step, depending on the type of investigation, but it would never be the first priority. Issuing a litigation hold to all affected parties might be a necessary step early on in an investigation of certain types, but not the first priority.

QUESTION 482
When creating a forensic image of a hard drive, which of the following should be the FIRST step?

A. Identify a recognized forensics software tool to create the image.
B. Establish a chain of custody log.
C. Connect the hard drive to a write blocker.
D. Generate a cryptographic hash of the hard drive contents.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The first step in any investigation requiring the creation of a forensic image should always be to maintain the chain of custody. Identifying a recognized forensics software tool to create the image is one of the important steps, but it should come after several of the other options. Connecting the hard drive to a write blocker is an important step, but it must be done after the chain of custody has been established. Generating a cryptographic hash of the hard drive contents is another important step, but one that comes after several of the other options.

QUESTION 483
Which of the following is the **MOST** effective way to detect information security incidents?

A. Providing regular and up-to-date training for the incident response team
B. Establishing proper policies for response to threats and vulnerabilities
C. Performing regular testing of the incident response program
D. Educating and users on threat awareness and timely reporting

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:

QUESTION 484
Which of the following is **MOST** important to verify when reviewing the effectiveness of response to an information security incident?

A. Lessons learned have been implemented.
B. Testing has been completed on time.
C. Test results have been properly recorded.
D. Metrics have been captured in a dashboard.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 485
The **PRIMARY** focus of a training curriculum for members of an incident response team should be:

A. specific role training
B. external corporate communication
C. security awareness
D. technology training

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 486
The **BEST** way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

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

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 487
Which of the following is **MOST** important for the effectiveness of an incident response function?

A. Enterprise security management system and forensic tools.
B. Establishing prior contacts with law enforcement
C. Training of all users on when and how to report
D. Automated incident tracking and reporting tools

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 488
Which of the following is the **MOST** important reason to consider the role of the IT service disk when developing incident handling procedures?

A. Service desk personnel have information on how to resolve common systems issues.
B. The service desk provides a source for the identification of security incidents.
C. The service desk provides information to prioritize systems recovery based on user.
D. Untrained service desk personnel may be a cause of security incidents.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 489
Which of the following is the **PRIMARY** responsibility of the designated spokesperson during incident response testing?

A. Communicating the severity of the incident to the board
B. Establishing communication channels throughout the organization
C. Evaluating the effectiveness of the communication processes
D. Acknowledging communications from the incident response team

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 490
Which of the following **BEST** contributes to the successful management of security incidents?

A. Established procedures
B. Established policies
C. Tested controls
D. Current technologies

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 491
After the occurrence of a major information security incident, which of the following will **BEST** help an information security manager determine corrective actions?

A. Calculating cost of the incident
B. Conducting a postmortem assessment
C. Preserving the evidence
D. Performing am impact analysis

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 492
Which of the following metrics is **MOST** appropriate for evaluating the incident notification process?

A. Average total cost of downtime per reported incident
B. Average number of incidents per reporting period

C. Elapsed time between response and resolution
D. Elapsed time between detection, reporting and response

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 493
It is suspected that key e-mails have been viewed by unauthorized parties. The e-mail administrator conducted an investigation but it has not returned any information relating to the incident, and leaks are continuing. Which of the following is the **BEST** recommended course of action to senior management?

A. Commence security training for staff at the organization.
B. Arrange for an independent review.
C. Rebuild the e-mail application.
D. Restrict the distribution of confidential e-mails.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 494
Which of the following be **MOST** effective in reducing the financial impact following a security breach leading to data disclosure?

A. A business continuity plan
B. Backup and recovery strategy
C. A data loss prevention (DLP) solution
D. An incident response plan

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 495
Which of the following **BEST** facilitates the effective execution of an incident response plan?

A. The response team is trained on the plan.
B. The plan is based on risk assessment results.
C. The incident response plan aligns with the IT disaster recovery plan.
D. The plan is based on industry best practice.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 496
An information security manager developing an incident response plan **MUST** ensure it includes:

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

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 497
In a cloud technology environment, which of the following would pose the **GREATEST** challenge to the investigation of security incidents?

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 498
What is the **MAIN** reason for an organization to develop an incident response plan?

A. Trigger immediate recovery procedures.
B. Identify training requirements for the incident response team.
C. Prioritize treatment based on incident criticality.
D. Provide a process for notifying stakeholders of the incident.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 499
Who is **MOST** important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data loss?

A. An independent auditor for identification of control deficiencies
B. A damage assessment expert for calculating losses
C. A forensics expert for evidence management
D. A penetration tester to validate the attack

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 500
Which of the following is the **PRIMARY** purpose of establishing an information security governance framework?

A. To minimize security risks
B. To proactively address security objectives
C. To reduce security audit issues
D. To enhance business continuity planning

Correct Answer: A

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 501
When developing an escalation process for an incident response plan, the information security manager should **PRIMARILY** consider the:

A. media coverage.
B. availability of technical resources.
C. incident response team.
D. affected stakeholders.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 502
Which of the following would be the **BEST** way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

A. Perform a penetration test to demonstrate the ability to protect.
B. Perform industry research annually and document the overall ranking of the IPS.
C. Establish and present appropriate metrics that track performance.
D. Provide yearly competitive pricing to illustrate the value of the IPS.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 503
An organization utilizes a third party to classify its customers' personally identifiable information (PII). What is the **BEST** way to hold the third party accountable for data leaks?

A. Include detailed documentation requirements within the formal statement of work.
B. Submit a formal request for proposal (RFP) containing detailed documentation of requirements.
C. Ensure a nondisclosure agreement is signed by both parties' senior management.
D. Require the service provider to sign off on the organization's acceptable use policy.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 504
When designing security controls, it is **MOST** important to:

A. apply a risk-based approach.
B. focus on preventive controls.
C. evaluate the costs associated with the controls.
D. apply controls to confidential information.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 505
Information classification is a fundamental step in determining:

A. whether risk analysis objectives are met.
B. who has ownership of information.
C. the type of metrics that should be captured.
D. the security strategy that should be used.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 506
Which of the following should be the **MOST** important consideration of business continuity management?

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 507
Which of the following would be **MOST** helpful when justifying the funding required for a compensating control?

A. Business case
B. Risk analysis
C. Business impact analysis
D. Threat assessment

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 508
Which of the following would **MOST** effectively ensure that information security is implemented in a new system?

A. Security baselines
B. Security scanning
C. Secure code reviews
D. Penetration testing

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 509
Which of the following is the **MOST** important component of information security governance?
A. Approved Information security strategy
B. Documented information security policies
C. Comprehensive information security awareness program
D. Appropriate information security metrics

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 510
A penetration test was conducted by an accredited third party. Which of the following should be the information security manager's **FIRST** course of action?

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

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 511
Which of the following functions is **MOST** critical when initiating the removal of system access for terminated employees?

A. Legal
B. Information security
C. Help desk

D. Human resources

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation
Explanation/Reference:

QUESTION 512
Which of the following is the **MOST** effective approach for delivering security incident response training?

A. Perform role-playing exercises to simulate real-world incident response scenarios.
B. Engage external consultants to present real-world examples within the industry.
C. Include incident response training within new staff orientation.
D. Provide on-the-job training and mentoring for the incident response team.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 513
Which of the following is **MOST** important to the successful development of an information security strategy?

A. A well-implemented governance framework
B. Current state and desired objectives
C. An implemented development life cycle process
D. Approved policies and standards

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 514
An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is **MOST** important to:

A. prohibit remote access to the site.
B. periodically recertify access rights.
C. enforce document lifecycle management.
D. conduct a vulnerability assessment.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 515
When aligning an organization's information security program with other risk and control activities, it is **MOST** important to:

A. develop an information security governance framework.
B. have information security management report to the chief risk officer.
C. ensure adequate financial resources are available.
D. integrate security within the system development life cycle.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 516
A large number of exceptions to an organization's information security standards have been granted after senior management approved a bring your own device (BYOD) program. To address this situation, it is **MOST** important for the information security manager to:

A. introduce strong authentication on devices.
B. reject new exception requests.
C. update the information security policy.
D. require authorization to wipe lost devices.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 517
Which of the following is the **PRIMARY** responsibility of the information security manager when an organization implements the use of personally-owned devices on the corporate network?

A. Requiring remote wipe capabilities
B. Enforcing defined policy and procedures
C. Conducting security awareness training
D. Encrypting the data on mobile devices

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 518
During an information security audit, it was determined that IT staff did not follow the established standard when configuring and managing IT systems. Which of the following is the **BEST** way to prevent future occurrences?

A. Updating configuration baselines to allow exceptions
B. Conducting periodic vulnerability scanning
C. Providing annual information security awareness training
D. Implementing a strict change control process

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 519
Which of the following should be the **PRIMARY** focus of a post-incident review following a successful response to a cybersecurity incident?

A. Which control failures contributed to the incident
B. How incident response processes were executed
C. What attack vectors were utilized

D. When business operations were restored

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 520
An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The **PRIMARY** purpose of this analysis should be to:

A. prepare for criminal prosecution.
B. document lessons learned.
C. evaluate the impact.
D. update information security policies.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 521
Which of the following is the **MOST** important reason for performing a cost-benefit analysis when implementing a security control?

A. To present a realistic information security budget
B. To ensure that benefits are aligned with business strategies
C. To ensure that the mitigation effort does not exceed the asset value
D. To justify information security program activities

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 522
An information security manager determines the organization's critical systems may be vulnerable to a new zero-day attack. The **FIRST** course of action is to:

A. advise management of risk and remediation cost.
B. analyze the probability of compromise.
C. survey peer organizations to see how they have addressed the issue.
D. re-assess the firewall configuration.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 523
Who should determine data access requirements for an application hosted at an organization's data center?

A. Business owner
B. Information security manager
C. Systems administrator
D. Data custodian

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 524
When conducting a post-incident review, the **GREATEST** benefit of collecting mean time to resolution (MTTR) data is the ability to:

A. reduce the costs of future preventive controls.
B. provide metrics for reporting to senior management.
C. learn of potential areas of improvement.
D. verify compliance with the service level agreement (SLA).

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 525
Which of the following provides the **MOST** relevant information to determine the overall effectiveness of an information security program and underlying business processes?

A. Balanced scorecard
B. Cost-benefit analysis
C. Industry benchmarks
D. SWOT analysis

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 526
Which of the following is the **FIRST** step to perform before outsourcing critical information processing to a third party?

A. Require background checks for third-party employees.
B. Perform a risk assessment.
C. Ensure that risks are formally accepted by third party.
D. Negotiate a service level agreement.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 527
Which of the following should occur **FIRST** in the process of managing security risk associated with the transfer of data from unsupported legacy systems to supported systems?

A. Make backups of the affected systems prior to transfer.
B. Increase cyber insurance coverage.

C. Identify all information assets in the legacy environment.
D. Assign owners to be responsible for the transfer of each asset.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 528
When reviewing the security controls of an application service provider, an information security manager discovers the provider's change management controls are insufficient. Changes to the provided application often occur spontaneously with no notification to clients. Which of the following would **BEST** facilitate a decision to continue or discontinue services with this provider?

A. Comparing the client organization's risk appetite to the disaster recovery plan of the service provider.
B. Comparing the client organization's risk appetite to the criticality of the supplied application. C. Comparing the client organization's risk appetite to the frequency of application downtimes.
D. Comparing the client organization's risk appetite to the vendor's change control policy.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 529
An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the **BEST** assurance that the third party's contract programmers comply with the organization's security policies? A. Require annual signed agreements of adherence to security policies.

B. Include penalties for noncompliance in the contracting agreement.
C. Perform periodic security assessments of the contractors' activities.
D. Conduct periodic vulnerability scans of the application.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 530
Which of the following is a **PRIMARY** function of an incident response team?

A. To provide a business impact assessment
B. To provide effective incident mitigation
C. To provide a single point of contact for critical incidents
D. To provide a risk assessment for zero-day vulnerabilities

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: