CISM.exam.370q

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

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

A. Defining and ratifying the classification structure of information assets
B. Deciding the classification levels applied to the organization's information assets
C. Securing information assets in accordance with their classification
D. Checking if information assets have been classified properly

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

QUESTION 2

Logging is an example of which type of defense against systems compromise?

A. Containment
B. DetectionC. Reaction
D. Recovery

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

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

QUESTION 3
Which of the following is MOST important in developing a security strategy?

A. Creating a positive business security environment
B. Understanding key business objectives
C. Having a reporting line to senior management
D. Allocating sufficient resources to information security

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

QUESTION 4
Who is ultimately responsible for the organization's information?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE Explanation

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

QUESTION 5
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

A. Alignment with industry best practices
B. Business continuity investment
C. Business benefits
D. Regulatory compliance

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 6
A security manager meeting the requirements for the international flow of personal data will need to ensure:

A. a data processing agreement.
B. a data protection registration.
C. the agreement of the data subjects.

D. subject access procedures.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

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

QUESTION 7
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

A. Ethics
B. Proportionality
C. Integration
D. Accountability

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 8
Which of the following is the MOST important prerequisite for establishing information security management within an organization?

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

D. Information security policy

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE Explanation

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

QUESTION 9
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees
B. Distance between physical locations
C. Complexity of organizational structure
D. Organizational budget

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 10
In order to highlight to management, the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 11
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

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

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 12
An outcome of effective security governance is:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 13
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

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

Correct Answer: D

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 14
Who should drive the risk analysis for an organization?

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 15
The FIRST step in developing an information security management program is to:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 16
Which of the following is the MOST important to keep in mind when assessing the value of information?

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

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

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

QUESTION 17
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 18
To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 19
Which of the following situations would MOST inhibit the effective implementation of security governance?

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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 20
To achieve effective strategic alignment of security initiatives, it is important that:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 21
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

A. Compliance with international security standards.
B. Use of a two-factor authentication system.

C. Existence of an alternate hot site in case of business disruption.
D. Compliance with the organization's information security requirements.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 22
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

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

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

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

QUESTION 23
The MOST useful way to describe the objectives in the information security strategy is through:

A. attributes and characteristics of the 'desired state."

B. overall control objectives of the security program.
C. mapping the IT systems to key business processes.
D. calculation of annual loss expectations.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 24
In order to highlight to management, the importance of network security, the security manager should FIRST:

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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

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

QUESTION 25
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions

C. Organization chart
D. Skills inventory

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 26
The MOST important characteristic of good security policies is that they:

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

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

QUESTION 27
An information security manager must understand the relationship between information security and business operations in order to:

A. support organizational objectives.

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

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 28
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

A. escalate issues to an external third party for resolution.
B. ensure that senior management provides authority for security to address the issues.
C. insist that managers or units not in agreement with the security solution accept the risk.
D. refer the issues to senior management along with any security recommendations.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Senior management is in the best position to arbitrate since they will look at the overall needs of the business in reaching a decision. The authority may be delegated to others by senior management after their review of the issues and security recommendations. Units should not be asked to accept the risk without first receiving input from senior management.

QUESTION 29
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

A. establishing a periodic risk assessment.
B. promoting regulatory requirements.
C. developing a business case.
D. developing effective metrics.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:

Business case development, including a cost-benefit analysis, will be most persuasive to management. A risk assessment may be included in the business ease, but by itself will not be as effective in gaining management support. Informing management of regulatory requirements may help gain support for initiatives, but given that more than half of all organizations are not in compliance with regulations, it is unlikely to be sufficient in many cases. Good metrics which provide assurance that initiatives are meeting organizational goals will also be useful, but are insufficient in gaining management support.

QUESTION 30
Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

A. Include security responsibilities in the job description
B. Require the administrator to obtain security certification
C. Train the system administrator on penetration testing and vulnerability assessment
D. Train the system administrator on risk assessment

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE Explanation

Explanation/Reference:
Explanation:
The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

QUESTION 31

Which of the following is the MOST important element of an information security strategy?

A. Defined objectives

B. Time frames for delivery
C. Adoption of a control framework
D. Complete policies

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Without defined objectives, a strategy — the plan to achieve objectives — cannot be developed. Time frames for delivery are important but not critical for inclusion in the strategy document. Similarly, the adoption of a control framework is not critical to having a successful information security strategy. Policies are developed subsequent to, and as a part of, implementing a strategy.

QUESTION 32
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 33
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 34
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 35
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 36
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 37

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 38

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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precise.
B. security risks are subject to frequent change.

C. reviewers can optimize and reduce the cost of controls.
D. it demonstrates to senior management that the security function can add value.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 49
Which of the following BEST indicates a successful risk management practice?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 50
Which of the following would generally have the GREATEST negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services

C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 51
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 52
Which of the following will BEST protect an organization from internal security attacks?

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

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

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

QUESTION 53
For risk management purposes, the value of an asset should be based on:

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 54
In a business impact analysis, the value of an information system should be based on the overall cost:

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 55
Acceptable risk is achieved when:

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 56
The value of information assets is BEST determined by:

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT Explanation

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

QUESTION 57
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 58
The MOST effective way to incorporate risk management practices into existing production systems is through:

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 59
Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 60
The recovery time objective (RTO) is reached at which of the following milestones?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 61
Which of the following results from the risk assessment process would BEST assist risk management decision making?

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 62
The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

A. Mitigating controls
B. Visibility of impact
C. Likelihood of occurrence
D. Incident frequency

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

QUESTION 63
Risk acceptance is a component of which of the following?
A. Assessment
B. Mitigation
C. EvaluationD. Monitoring

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

QUESTION 64
Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.
B. the point at which the benefit exceeds the expense.
C. a level that the organization is willing to accept.
D. a rate of return that equals the current cost of capital.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

QUESTION 65
A risk assessment should be conducted:

A. once a year for each business process and subprocess.
B. every three to six months for critical business processes.
C. by external parties to maintain objectivity.
D. annually or whenever there is a significant change.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

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.

QUESTION 82
The PRIMARY objective of a risk management program is to:

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 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, 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:

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 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.
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)
B. Maximum tolerable outage (MTO)
C. Recovery point objectives (RPOs)
D. Services delivery objectives (SDOs)

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

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

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 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.

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.
C. the cost of countermeasure outweighs the value of the asset and potential loss.
D. The likelihood of the risk occurring is unknown.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 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:

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 results
C. Customer personal information
D. Previous financial results

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 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

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

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 124
Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

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

QUESTION 125

One way to determine control effectiveness is by determining:

A. whether it is preventive, detective or compensatory.
B. the capability of providing notification of failure.
C. the test results of intended objectives.
D. the evaluation and analysis of reliability.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

QUESTION 126
What does a network vulnerability assessment intend to identify?

A. 0-day vulnerabilities
B. Malicious software and spyware
C. Security design flaws
D. Misconfiguration and missing updates

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

A network vulnerability assessment intends to identify known vulnerabilities based on common misconfigurations and missing updates. 0-day vulnerabilities by definition are not previously known and therefore are undetectable. Malicious software and spyware are normally addressed through antivirus and antispyware policies. Security design flaws require a deeper level of analysis.

QUESTION 127

Who is responsible for ensuring that information is classified?

A. Senior management
B. Security manager
C. Data owner
D. Custodian

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

QUESTION 128
After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

A. transferred.
B. treated.
C. accepted.
D. terminated.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

When the cost of control is more than the cost of the risk, the risk should be accepted. Transferring, treating or terminating the risk is of limited benefit if the cost of that control is more than the cost of the risk itself.

QUESTION 129
When a significant security breach occurs, what should be reported FIRST to senior management?

A. A summary of the security logs that illustrates the sequence of events
B. An explanation of the incident and corrective action taken
C. An analysis of the impact of similar attacks at other organizations
D. A business case for implementing stronger logical access controls

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

When reporting an incident to senior management, the initial information to be communicated should include an explanation of what happened and how the breach was resolved. A summary of security logs would be too technical to report to senior management. An analysis of the impact of similar attacks and a business case for improving controls would be desirable; however, these would be communicated later in the process.

QUESTION 130
The PRIMARY reason for initiating a policy exception process is when:

A. operations are too busy to comply.
B. the risk is justified by the benefit.
C. policy compliance would be difficult to enforce.
D. users may initially be inconvenienced.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Exceptions to policy are warranted in circumstances where compliance may be difficult or impossible and the risk of noncompliance is outweighed by the benefits. Being busy is not a justification for policy exceptions, nor is the fact that compliance cannot be enforced. User inconvenience is not a reason to automatically grant exception to a policy.

QUESTION 131
Which of (lie following would be the MOST relevant factor when defining the information classification policy?

A. Quantity of information
B. Available IT infrastructure
C. Benchmarking
D. Requirements of data owners

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

When defining the information classification policy, the requirements of the data owners need to be identified. The quantity of information, availability of IT infrastructure and benchmarking may be part of the scheme after the fact and would be less relevant.

QUESTION 132
To determine the selection of controls required to meet business objectives, an information security manager should:

A. prioritize the use of role-based access controls.
B. focus on key controls.
C. restrict controls to only critical applications.
D. focus on automated controls.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

QUESTION 133
The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

A. sales department.
B. database administrator.
C. chief information officer (CIO).

D. head of the sales department.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The owner of the information asset should be the person with the decision-making power in the department deriving the most benefit from the asset. In this case, it would be the head of the sales department. The organizational unit cannot be the owner of the asset because that removes personal responsibility. The database administrator is a custodian. The chief information officer (CIO) would not be an owner of this database because the CIO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

QUESTION 134
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

A. develop an operational plan for achieving compliance with the legislation.
B. identify systems and processes that contain privacy components.
C. restrict the collection of personal information until compliant.
D. identify privacy legislation in other countries that may contain similar requirements.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Identifying the relevant systems and processes is the best first step. Developing an operational plan for achieving compliance with the legislation is incorrect because it is not the first step. Restricting the collection of personal information comes later. Identifying privacy legislation in other countries would not add much value.

QUESTION 135
Risk assessment is MOST effective when performed:

A. at the beginning of security program development.
B. on a continuous basis.
C. while developing the business case for the security program.
D. during the business change process.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

QUESTION 136
Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

A. Justification of the security budget must be continually made.
B. New vulnerabilities are discovered every day.
C. The risk environment is constantly changing.
D. Management needs to be continually informed about emerging risks.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The risk environment is impacted by factors such as changes in technology, and business strategy. These changes introduce new threats and vulnerabilities to the organization. As a result, risk assessment should be performed continuously. Justification of a budget should never be the main reason for performing a risk assessment. New vulnerabilities should be managed through a patch management process. Informing management about emerging risks is important, but is not the main driver for determining when a risk assessment should be performed.

QUESTION 137
There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

A. Identify the vulnerable systems and apply compensating controls
B. Minimize the use of vulnerable systems
C. Communicate the vulnerability to system users
D. Update the signatures database of the intrusion detection system (IDS)

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The best protection is to identify the vulnerable systems and apply compensating controls until a patch is installed. Minimizing the use of vulnerable systems and communicating the vulnerability to system users could be compensating controls but would not be the first course of action. Choice D does not make clear the timing of when the intrusion detection system (IDS) signature list would be updated to accommodate the vulnerabilities that are not yet publicly known. Therefore, this approach should not always be considered as the first option.

QUESTION 138
Which of the following devices should be placed within a DMZ?

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

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 139
An intrusion detection system should be placed:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 140
The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 141
An extranet server should be placed:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 142
Which of the following is the BEST metric for evaluating the effectiveness of security awareness twining? The number of:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 143
Security monitoring mechanisms should PRIMARILY:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 144
Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 145

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

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 146

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

A. Number of attacks detected
B. Number of successful attacks
C. Ratio of false positives to false negatives
D. Ratio of successful to unsuccessful attacks

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 147

Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

A. Patch management

B. Change management

C. Security baselines
D. Virus detection

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 148
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart
C. Critical path
D. Rapid Application Development (RAD)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 149
Which of the following is MOST effective in preventing security weaknesses in operating systems?

A. Patch management Change
management

B.

C. Security baselines
D. Configuration management

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 150
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 151
Who can BEST approve plans to implement an information security governance framework?

A. Internal auditor
B. Information security management
Steering committee
C.

D. Infrastructure management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 152
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 153
Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

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

D.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 154
Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 155
Which of the following devices should be placed within a demilitarized zone (DMZ)?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 156
On which of the following should a firewall be placed?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 157
An intranet server should generally be placed on the:

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

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

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

QUESTION 158

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

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 159

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 160

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 161

The information classification scheme should:

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

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 162
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 163
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 164
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 165
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 166
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 167
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 168
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 169
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 170
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 171
Which of the following is MOST important to the success of an information security program?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 172
Which of the following is MOST important for a successful information security program?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 173
Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

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

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

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

QUESTION 174
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 175
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 176
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 177
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 178

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 179

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 180
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 181
The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 182
Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have his, her password reset?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 183
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 184
The BEST way to ensure that an external service provider complies with organizational security policies is to:

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 185
When an emergency security patch is received via electronic mail, the patch should FIRST be:

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

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

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

QUESTION 186
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 187
Which of the following is the BEST indicator that security awareness training has been effective?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 188

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

A. Penetration attempts investigated
B. Violation log reports produced
C. Violation log entries
D. Frequency of corrective actions taken

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 189
Which of the following change management activities would be a clear indicator that normal operational procedures require examination? A high percentage of:

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

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

QUESTION 190
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 191
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 192
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 193
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 194
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 195
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 196
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 197

Which of the following areas is MOST susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management
C. Configuration management
D. Incident response management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Configuration management provides the greatest likelihood of security weaknesses through misconfiguration and failure to update operating system (OS) code correctly and on a timely basis.

QUESTION 198
Security policies should be aligned MOST closely with:

A. industry' best practices.
B. organizational needs.
C. generally accepted standards.
D. local laws and regulations.

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

The needs of the organization should always take precedence. Best practices and local regulations are important, but they do not take into account the total needs of an organization.

QUESTION 199
The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performance.
B. use a honeypot to check for unusual activity.
C. audit the configuration of the IDS.

D. benchmark the IDS against a peer site.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Simulating an attack on the network demonstrates whether the intrusion detection system (IDS) is properly tuned. Reviewing the configuration may or may not reveal weaknesses since an anomaly-based system uses trends to identify potential attacks. A honeypot is not a good first step since it would need to have already been penetrated. Benchmarking against a peer site would generally not be practical or useful.

QUESTION 200
The BEST time to perform a penetration test is after:

A. an attempted penetration has occurred.
B. an audit has reported weaknesses in security controls.
C. various infrastructure changes are made.
D. a high turnover in systems staff.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Changes in the systems infrastructure are most likely to inadvertently introduce new exposures. Conducting a test after an attempted penetration is not as productive since an organization should not wait until it is attacked to test its defenses. Any exposure identified by an audit should be corrected before it would be appropriate to test. A turnover in administrative staff does not warrant a penetration test, although it may- warrant a review of password change practices and configuration management.

QUESTION 201
Successful social engineering attacks can BEST be prevented through:

A. preemployment screening.
B. close monitoring of users' access patterns.
C. periodic awareness training.
D. efficient termination procedures.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

QUESTION 202
What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

A. Perform periodic penetration testing
B. Establish minimum security baselines
C. Implement vendor default settings
D. Install a honeypot on the network

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed sporadically. Vendor default settings are not effective.

QUESTION 203
Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

A. User ad hoc reporting is not logged
B. Network traffic is through a single switch
C. Operating system (OS) security patches have not been applied
D. Database security defaults to ERP settings

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security-weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

QUESTION 204
In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

A. Implementing on-screen masking of passwords
B. Conducting periodic security awareness programs
C. Increasing the frequency of password changes
D. Requiring that passwords be kept strictly confidential

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

Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt. Implementing on-screen masking of passwords and increasing the frequency of password changes are desirable, but these will not be effective in reducing the likelihood of a successful social engineering attack. Requiring that passwords be kept secret in security policies is a good control but is not as effective as periodic security awareness programs that will alert users of the dangers posed by social engineering.

QUESTION 205

Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security-steering committees
D. Security awareness campaigns

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self- assessment exercises are all good but do not exemplify the taking of ownership by management.

QUESTION 206
Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System analyst
B. Quality control manager
C. Process owner
D. Information security manager

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

QUESTION 207
What is the BEST way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards

B. Have the contractors acknowledge in writing the security policies
C. Create penalties for noncompliance in the contracting agreement
D. Perform periodic security reviews of the contractors

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Periodic reviews are the most effective way of obtaining compliance. None of the other options detects the failure of contract programmers to comply.

QUESTION 208
Which of the following activities is MOST likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

If malicious code is not immediately detected, it will most likely be backed up as a part of the normal tape backup process. When later discovered, the code may be eradicated from the device but still remain undetected ON a backup tape. Any subsequent restores using that tape may reintroduce the malicious code. Applying patches, changing access rules and upgrading hardware does not significantly increase the level of difficulty.

QUESTION 209
Security awareness training should be provided to new employees:

A. on an as-needed basis.
B. during system user training.
C. before they have access to data.
D. along with department staff.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Security awareness training should occur before access is granted to ensure the new employee understands that security is part of the system and business process. All other choices imply that security awareness training is delivered subsequent to the granting of system access, which may place security as a secondary step.

QUESTION 210
What is the BEST method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to operating system (OS) patch logs
B. Trace OS patch logs to OS vendor's update documentation
C. Trace OS patch logs to change control requests
D. Review change control documentation for key servers

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

To ensure that all patches applied went through the change control process, it is necessary to use the operating system (OS) patch logs as a starting point and then check to see if change control documents are on file for each of these changes. Tracing from the documentation to the patch log will not indicate if some patches were applied without being documented. Similarly, reviewing change control documents for key servers or comparing patches applied to those recommended by the OS vendor's web site does not confirm that these security patches were properly approved and documented.

QUESTION 211
A security awareness program should:

A. present top management's perspective.
B. address details on specific exploits.
C. address specific groups and roles.
D. promote security department procedures.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Different groups of employees have different levels of technical understanding and need awareness training that is customized to their needs; it should not be presented from a specific perspective. Specific details on technical exploits should be avoided since this may provide individuals with knowledge they might misuse or it may confuse the audience. This is also not the best forum in which to present security department procedures.

QUESTION 212
The PRIMARY objective of security awareness is to:

A. ensure that security policies are understood.
B. influence employee behavior.
C. ensure legal and regulatory compliance
D. notify of actions for noncompliance.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, or meeting legal and regulatory requirements is important but secondary.

QUESTION 213
Which of the following will BEST protect against malicious activity by a former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important, but are not as effective in preventing this type of situation.

QUESTION 214
Which of the following represents a PRIMARY area of interest when conducting a penetration test?

A. Data mining
B. Network mapping
C. Intrusion Detection System (IDS)
D. Customer data

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Network mapping is the process of determining the topology of the network one wishes to penetrate. This is one of the first steps toward determining points of attack in a network. Data mining is associated with ad hoc reporting and. together with customer data, they are potential targets after the network is penetrated. The intrusion detection mechanism in place is not an area of focus because one of the objectives is to determine how effectively it protects the network or how easy it is to circumvent.

QUESTION 215
The return on investment of information security can BEST be evaluated through which of the following?

A. Support of business objectives
B. Security metrics
C. Security deliverables
D. Process improvement models

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

One way to determine the return on security investment is to illustrate how information security supports the achievement of business objectives. Security metrics measure improvement and effectiveness within the security practice but do not tie to business objectives. Similarly, listing deliverables and creating process improvement models does not necessarily tie into business objectives.

QUESTION 216

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

A. set their accounts to expire in six months or less.
B. avoid granting system administration roles.
C. ensure they successfully pass background checks.
D. ensure their access is approved by the data owner.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Contract personnel should not be given job duties that provide them with power user or other administrative roles that they could then use to grant themselves access to sensitive files. Setting expiration dates, requiring background checks and having the data owner assign access are all positive elements, but these will not prevent contract personnel from obtaining access to sensitive information.

QUESTION 217

Information security policies should:

A. address corporate network vulnerabilities.
B. address the process for communicating a violation.
C. be straightforward and easy to understand.
D. be customized to specific groups and roles.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

As high-level statements, information security policies should be straightforward and easy to understand. They arc high-level and, therefore, do not address network vulnerabilities directly or the process for communicating a violation. As policies, they should provide a uniform message to all groups and user roles.

QUESTION 218
Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection system.
B. Establish minimum security baselines.
C. Implement vendor recommended settings.
D. Perform periodic penetration testing.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Penetration testing is the best way to assure that perimeter security is adequate. An intrusion detection system (IDS) may detect an attempted attack, hut it will not confirm whether the perimeter is secured. Minimum security baselines and applying vendor recommended settings are beneficial, but they will not provide the level of assurance that is provided by penetration testing.

QUESTION 219
Which of the following presents the GREATEST exposure to internal attack on a network?

A. User passwords are not automatically expired
B. All network traffic goes through a single switch
C. User passwords are encoded but not encrypted
D. All users reside on a single internal subnet

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

When passwords are sent over the internal network in an encoded format, they can easily be converted to clear text. All passwords should be encrypted to provide adequate security. Not automatically expiring user passwords does create an exposure, but not as great as having unencrypted passwords. Using a single switch or subnet does not present a significant exposure.

QUESTION 220
Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

A. Standards
B. Guidelines
C. Security metricsD. IT governance

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Standards are the bridge between high-level policy statements and the "how to" detailed formal of procedures. Security metrics and governance would not ensure correct alignment between policies and procedures. Similarly, guidelines are not linkage documents but rather provide suggested guidance on best practices.

QUESTION 221
Which of the following are the MOST important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer
B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal departments

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Security steering committees provide a forum for management to express its opinion and take some ownership in the decision making process. It is imperative that business process owners be included in this process. None of the other choices includes input by business process owners.

QUESTION 222
Security audit reviews should PRIMARILY:

A. ensure that controls operate as required.
B. ensure that controls are cost-effective.
C. focus on preventive controls.
D. ensure controls are technologically current.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

The primary objective of a security review or audit should be to provide assurance on the adequacy of security controls. Reviews should focus on all forms of control, not just on preventive control. Cost-effectiveness and technological currency are important but not as critical.

QUESTION 223
Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting; in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

QUESTION 224
What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

A. Mandatory
B. Discretionary
C. Walled garden
D. Role-based

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Mandatory access controls restrict access to files based on the security classification of the file. This prevents users from sharing files with unauthorized users. Role-based access controls grant access according to the role assigned to a user; they do not prohibit file sharing. Discretionary and lattice-based access controls are not as effective as mandatory access controls in preventing file sharing. A walled garden is an environment that controls a user's access to web content and services. In effect, the walled garden directs the user's navigation within particular areas, and does not necessarily prevent sharing of other material.

QUESTION 225
Which of the following is an inherent weakness of signature-based intrusion detection systems?

A. A higher number of false positives
B. New attack methods will be missed
C. Long duration probing will be missed D. Attack profiles can be easily spoofed

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

QUESTION 226
Data owners are normally responsible for which of the following?

A. Applying emergency changes to application data
B. Administering security over database records
C. Migrating application code changes to production
D. Determining the level of application security required

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Data owners approve access to data and determine the degree of protection that should be applied (data classification). Administering database security, making emergency changes to data and migrating code to production are infrastructure tasks performed by custodians of the data.

QUESTION 227
Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

A. System analyst
B. System user
C. Operations manager
D. Data security officer

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

System users, specifically the user acceptance testers, would be in the best position to note whether new exposures are introduced during the change management process. The system designer or system analyst, data security officer and operations manager would not be as closely involved in testing code changes.

QUESTION 228
What is the BEST way to ensure users comply with organizational security requirements for password complexity?

A. Include password construction requirements in the security standards
B. Require each user to acknowledge the password requirements
C. Implement strict penalties for user noncompliance

D. Enable system-enforced password configuration

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Automated controls are generally more effective in preventing improper actions. Policies and standards provide some deterrence, but are not as effective as automated controls.

QUESTION 229
Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

A. Batch patches into frequent server updates
B. Initially load the patches on a test machine
C. Set up servers to automatically download patches
D. Automatically push all patches to the servers

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Some patches can conflict with application code. For this reason, it is very important to first test all patches in a test environment to ensure that there are no conflicts with existing application systems. For this reason, choices C and D are incorrect as they advocate automatic updating. As for frequent server updates, this is an incomplete (vague) answer from the choices given.

QUESTION 230
Which of the following would present the GREATEST risk to information security?

A. Virus signature files updates are applied to all servers every day
B. Security access logs are reviewed within five business days
C. Critical patches are applied within 24 hours of their release
D. Security incidents are investigated within five business days

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT Explanation

Explanation/Reference:
Explanation:

Security incidents are configured to capture system events that are important from the security perspective; they include incidents also captured in the security access logs and other monitoring tools. Although, in some instances, they could wait for a few days before they are researched, from the options given this would have the greatest risk to security. Most often, they should be analyzed as soon as possible. Virus signatures should be updated as often as they become available by the vendor, while critical patches should be installed as soon as they are reviewed and tested, which could occur in 24 hours.

QUESTION 231
The PRIMARY reason for using metrics to evaluate information security is to:

A. identify security weaknesses.
B. justify budgetary expenditures.
C. enable steady improvement.
D. raise awareness on security issues.

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

The purpose of a metric is to facilitate and track continuous improvement. It will not permit the identification of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

QUESTION 232
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 233
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 234
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 235
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 236
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 237
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 238
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 239
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 240
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 241
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 242
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 243
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 244
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 245
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 246
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 247
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?

A. Enable access through a separate device that requires adequate authentication
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 248
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 249
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 250
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.

QUESTION 251
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 252

B.
In business-critical applications, user access should be approved by the:

A. information security manager.

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 253
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.

B.

QUESTION 254

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

A. end users.

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 255

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

B.
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 256
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 257
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 258
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 259
A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GREATEST weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks
B. The hot site may have to be shared with other customers
C. The time of declaration determines site access priority
D. The provider services all major companies in the area

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. Access to a hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

QUESTION 260
Which of the following actions should be taken when an online trading company discovers a network attack in progress?

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

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

QUESTION 261
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.
B. bastion hosts.
C. decoy files.
D. screened subnets.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

QUESTION 262
The FIRST priority when responding to a major security incident is:

A. documentation.
B. monitoring.
C. restoration.
D. containment.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

The first priority in responding to a security incident is to contain it to limit the impact. Documentation, monitoring and restoration are all important, but they should follow containment.

QUESTION 263
Which of the following is the MOST important to ensure a successful recovery?

A. Backup media is stored offsite
B. Recovery location is secure and accessible
C. More than one hot site is available
D. Network alternate links are regularly tested

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Unless backup media are available, all other preparations become meaningless. Recovery site location and security are important, but would not prevent recovery in a disaster situation. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, alternate data communication lines should be tested regularly and successfully but, again, this is not as critical.

QUESTION 264
Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot site?

B.

A. Tests are scheduled on weekends Network
IP addresses are predefined
C. Equipment at the hot site is identical
D. Business management actively participates

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Disaster recovery testing requires the allocation of sufficient resources to be successful. Without the support of management, these resources will not be available, and testing will suffer as a result. Testing on weekends can be advantageous but this is not the most important choice. As vendor-provided hot sites are in a state of constant change, it is not always possible to have network addresses defined in advance. Although it would be ideal to provide for identical equipment at the hot site, this is not always practical as multiple customers must be served and equipment specifications will therefore vary.

QUESTION 265
At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

A. Erase data and software from devices
B. Conduct a meeting to evaluate the test
C. Complete an assessment of the hot site provider
D. Evaluate the results from all test scripts

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations can occur back at the office after everyone is rested, and the overall results can be discussed and compared objectively.

QUESTION 266
An incident response policy must contain:

C.

A. updated call trees.
B. escalation criteria.
press release templates.
D. critical backup files inventory.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Escalation criteria, indicating the circumstances under which specific actions are to be undertaken, should be contained within an incident response policy. Telephone trees, press release templates and lists of critical backup files are too detailed to be included in a policy document.

QUESTION 267
The BEST approach in managing a security incident involving a successful penetration should be to:

A. allow business processes to continue during the response.
B. allow the security team to assess the attack profile.
C. permit the incident to continue to trace the source.
D. examine the incident response process for deficiencies.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted. Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable but it, too. is subordinate to allowing business processes to continue.

QUESTION 268
A post-incident review should be conducted by an incident management team to determine:

D.

A. relevant electronic evidence.
B. lessons learned.
C. hacker's identity.areas affected.

E.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Post-incident reviews are beneficial in determining ways to improve the response process through lessons learned from the attack. Evaluating the relevance of evidence, who launched the attack or what areas were affected are not the primary purposes for such a meeting because these should have been already established during the response to the incident.

QUESTION 269
An organization with multiple data centers has designated one of its own facilities as the recovery site. The MOST important concern is the:

A. communication line capacity between data centers.
B. current processing capacity loads at data centers.
C. differences in logical security at each center.
D. synchronization of system software release versions.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

If data centers are operating at or near capacity, it may prove difficult to recover critical operations at an alternate data center. Although line capacity is important from a mirroring perspective, this is secondary to having the necessary capacity to restore critical systems. By comparison, differences in logical and physical security and synchronization of system software releases are much easier issues to overcome and are, therefore, of less concern.

QUESTION 270
Which of the following is MOST important in determining whether a disaster recovery test is successful?

A. Only business data files from offsite storage are used
B. IT staff fully recovers the processing infrastructure
C. Critical business processes are duplicated
D. All systems are restored within recovery time objectives (RTOs)

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

To ensure that a disaster recovery test is successful, it is most important to determine whether all critical business functions were successfully recovered and duplicated. Although ensuring that only materials taken from offsite storage are used in the test is important, this is not as critical in determining a test's success. While full recovery of the processing infrastructure is a key recovery milestone, it does not ensure the success of a test. Achieving the RTOs is another important milestone, but does not necessarily prove that the critical business functions can be conducted, due to interdependencies with other applications and key elements such as data, staff, manual processes, materials and accessories, etc.

QUESTION 271
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

A. Cost to build a redundant processing facility and invocation
B. Daily cost of losing critical systems and recovery time objectives (RTOs)
C. Infrastructure complexity and system sensitivity
D. Criticality results from the business impact analysis (BIA)

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

The complexity and business sensitivity of the processing infrastructure and operations largely determines the viability of such an option; the concern is whether the recovery site meets the operational and security needs of the organization. The cost to build a redundant facility is not relevant since only a fraction of the total processing capacity is considered critical at the time of the disaster and recurring contract costs would accrue over time. Invocation costs are not a factor because they will be the same regardless. The incremental daily cost of losing different systems and the recovery time objectives (RTOs) do not distinguish whether a commercial facility is chosen. Resulting criticality from the business impact analysis (BIA) will determine the scope and timeline of the recovery efforts, regardless of the recovery location.

QUESTION 272
A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

A. Quarantine all picture files stored on file servers
B. Block all e-mails containing picture file attachments
C. Quarantine all mail servers connected to the Internet
D. Block incoming Internet mail, but permit outgoing mail

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Until signature files can be updated, incoming e-mail containing picture file attachments should be blocked. Quarantining picture files already stored on file servers is not effective since these files must be intercepted before they are opened. Quarantine of all mail servers or blocking all incoming mail is unnecessary overkill since only those e-mails containing attached picture files are in question.

QUESTION 273
When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall
B. Power down all servers located on the DMZ segment
C. Monitor the probe and isolate the affected segment
D. Enable server trace logging on the affected segment

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the demilitarized zone (DMZ) servers and enabling server trace routing are not warranted.

QUESTION 274
Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

A. A hot site facility will be shared in multiple disaster declarations

B. All equipment is provided "at time of disaster, not on floor"
C. The facility is subject to a "first-come, first-served" policy
D. Equipment may be substituted with equivalent model

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Equipment provided "at time of disaster (ATOD), not on floor" means that the equipment is not available but will be acquired by the commercial hot site provider ON a best effort basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations, and that priority may be established on a first-come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

QUESTION 275
Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite
B. Conduct an assessment to determine system status
C. Perform an impact analysis of the outage
D. Isolate the screened subnet

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

An assessment should be conducted to determine whether any permanent damage occurred and the overall system status. It is not necessary at this point to rebuild any servers. An impact analysis of the outage or isolating the demilitarized zone (DMZ) or screen subnet will not provide any immediate benefit.

QUESTION 276
Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

A. Detailed technical recovery plans are maintained offsite
B. Network redundancy is maintained through separate providers

C. Hot site equipment needs are recertified on a regular basis
D. Appropriate declaration criteria have been established

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

In a major disaster, staff can be injured or can be prevented from traveling to the hot site, so technical skills and business knowledge can be lost. It is therefore critical to maintain an updated copy of the detailed recovery plan at an offsite location. Continuity of the business requires adequate network redundancy, hot site infrastructure that is certified as compatible and clear criteria for declaring a disaster. Ideally, the business continuity program addresses all of these satisfactorily. However, in a disaster situation, where all these elements are present, but without the detailed technical plan, business recovery will be seriously impaired.

QUESTION 277
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 278
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 279
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 280
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 281
Which of the following actions should be taken when an information security manager discovers that a hacker is foot printing the network perimeter?

A. Reboot the border router connected to the firewall
B. Check IDS logs and monitor for any active attacks
C. Update IDS software to the latest available version
D. Enable server trace logging on the DMZ segment

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Information security should check the intrusion detection system (IDS) logs and continue to monitor the situation. It would be inappropriate to take any action beyond that. In fact, updating the IDS could create a temporary exposure until the new version can be properly tuned. Rebooting the router and enabling server trace routing would not be warranted.

QUESTION 282
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 283
Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m. (23.00 hrs.)?

A. Most new viruses* signatures are identified over weekends
B. Technical personnel are not available to support the operation
C. Systems are vulnerable to new viruses during the intervening week
D. The update's success or failure is not known until Monday

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Updating virus signature files on a weekly basis carries the risk that the systems will be vulnerable to viruses released during the week; far more frequent updating is essential. All other issues are secondary to this very serious exposure.

QUESTION 284
When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

A. Business continuity coordinator
B. Information security manager
C. Business process owners
D. Industry averages benchmarks

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Business process owners are in the best position to understand the true impact on the business that a system outage would create. The business continuity coordinator, industry averages and even information security will not be able to provide that level of detailed knowledge.

QUESTION 285
Which of the following is MOST closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy
C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
Explanation:

Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

QUESTION 286
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 287
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 288
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 289
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 290

Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications
B. Identification of network applications to be externally accessed
C. Identification of vulnerabilities associated with network applications to be externally accessed
D. Creation of an applications traffic matrix showing protection methods

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

QUESTION 291
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.
B. Specific user accountability cannot be established.
C. Unauthorized users may have access to originate, modify or delete data.
D. Audit recommendations may not be implemented.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

QUESTION 292

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized
B. Managed
C. Defined
D. Repeatable

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

QUESTION 293
When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

QUESTION 294

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A. A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
B. Firewall policies are updated on the basis of changing requirements.
C. inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all installation options.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

QUESTION 295
Which of the following is MOST critical for the successful implementation and maintenance of a security policy?
A. Assimilation of the framework and intent of a written security policy by all appropriate parties
B. Management support and approval for the implementation and maintenance of a security policy
C. Enforcement of security rules by providing punitive actions for any violation of security rules
D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the

importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

QUESTION 296

Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

QUESTION 297

Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

QUESTION 298

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

QUESTION 299
When segregation of duties concerns exists between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught.
Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

QUESTION 300
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

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

QUESTION 301
When considering whether to adopt a new information security framework, an organization's information security manager should FIRST:

A. compare the framework with the current business strategy
B. perform a technical feasibility analysis
C. perform a financial viability study
D. analyze the framework's legal implications and business impact

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 302
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 303
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 304
Which of the following BEST enables the deployment of consistent security throughout international branches within a multinational organization?
A. Maturity of security processes
B. Remediation of audit findings
C. Decentralization of security governance
D. Establishment of security governance

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 305

A data-hosting organization's data center houses servers, applications, and data for a large number of geographically dispersed customers. Which of the following strategies would be the BEST approach for developing a physical access control policy for the organization?

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

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 306
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 307
Which of the following would be MOST effective in the strategic alignment of security initiatives?

A. A security steering committee is set up within the IT department.
B. Key information security policies are updated on a regular basis.
C. Business leaders participate in information security decision making.
D. Policies are created with input from business unit managers.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 308

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 steering committees

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 309

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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 310

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

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

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

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

QUESTION 311
Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Ensure that proper controls exist for code review and release management
B. Set up an agent to run a virus-scanning program across platforms
C. Implement controls for continuous monitoring of middleware transactions
D. Apply the latest patch programs to the production operating systems

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 312
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 313
Security governance is MOST associated with which of the following IT infrastructure components?

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

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 314
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 315
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 316
When developing security standards, which of the following would be MOST appropriate to include?

A. Accountability for licenses
B. Acceptable use of IT assets
C. operating system requirements
D. Inventory management

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 317
During a post-incident review, the sequence and correlation of actions must be analyzed PRIMARILY based on:

A. documents created during the incident
B. logs from systems involved
C. a consolidated event time line
D. interviews with personnel

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 318
The BEST way to mitigate the risk associated with a social engineering attack is to:

A. deploy an effective intrusion detection system (IDS)
B. perform a user-knowledge gap assessment of information security practices
C. perform a business risk assessment of the email filtering system
D. implement multi-factor authentication on critical business systems

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 319
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 320
Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

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

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 321
A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:
A. contact the employees involved to retake security awareness training
B. notify senior management that employees are breaching policy
C. limit access to the Internet for employees involved
D. initiate an investigation to determine the full extent of noncompliance

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 322
An incident response team has determined there is a need to isolate a system that is communicating with a known malicious host on the Internet. Which of the following stakeholders should be contacted FIRST?

A. Key customers
B. Executive management
C. System administrator
D. The business owner

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 323
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: INCIDENT MANAGEMENT AND RESPONSE
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 324
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: INCIDENT MANAGEMENT AND RESPONSE 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 325
The MOST important element in achieving executive commitment to an information security governance program is:

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

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 326
To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

A. noncompliance issues are reported to senior management
B. information security management understands business performance issues
C. the security policy is changed to accommodate IT performance pressure
D. senior management provides guidance and dispute resolution

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 327
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 328
The BEST way to facilitate the reporting and escalation of potential security incidents to appropriate stakeholders is to define incident classifications based on the:

A. technique used to launch the attack
B. vulnerability exploited by the attack
C. verified source and industry rating of the incident
D. severity and impact of the incident

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 329
The business advantage of implementing authentication tokens is that they:

A. provide nonrepudiation
B. reduce overall cost
C. improve access security
D. reduce administrative workload

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 330
A contract bid is digitally signed and electronically mailed. The PRIMARY advantage to using a digital signature is that:

A. the bid and the signature can be copied from one document to another
B. the bid cannot be forged even if the keys are compromised
C. the signature can be authenticated even if no encryption is used
D. any alteration of the bid will invalidate the signature

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 331
As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain any effective information security program?

A. Ensure information security is included in any change control efforts
B. Merge the two information security programs to establish continuity
C. Determine new factors that could influence the information security strategy
D. Implement the current information security program in the acquired company

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 332

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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 333

An information security manager learns that a departmental system is out of compliance with the information security policy's password strength requirements. Which of the following should be the information security manager's FIRST course of action?

A. Submit the issue to the steering committee for escalation
B. Conduct an impact analysis to quantify the associated risk
C. Isolate the non-compliant system from the rest of the network
D. Request risk acceptance from senior management

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 334

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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 335
Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?

A. The business need for the function
B. The cost of the services
C. The vendor's reputation in the industry
D. The ability to meet deliverables

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 336
Which of the following BEST ensures timely and reliable access to services?

A. Authenticity
B. Recovery time objective
C. Availability
D. Nonrepudiation

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Reference https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

QUESTION 337
Which of the following would be MOST effective in ensuring that information security is appropriately addressed in new systems?

A. Internal audit signs off on security prior to implementation
B. Information security staff perform compliance reviews before production begins
C. Information security staff take responsibility for the design of system security
D. Business requirements must include security objectives

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 338
Of the following, whose input is of GREATEST importance in the development of an information security strategy?

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

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 339
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization’s information security strategy?

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 340
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: INCIDENT MANAGEMENT AND RESPONSE 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 341
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 342

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: INCIDENT MANAGEMENT AND RESPONSE 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 343

Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is MOST important for the information security manager to periodically:

A. perform a cost-benefit analysis
B. review firewall configuration

C. review the security policy
D. perform a risk assessment

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 344
Attacks using multiple methods to spread should be classified:

A. each time the exposure is experienced
B. depending on the method used to spread
C. at the highest potential level of business impact
D. using multiple classifications for each impact

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 345
A semi-annual disaster recovery test has been completed. Which of the following issues discussed during the lessons learned phase should be of GREATEST concern?

A. A server used in recovery did not have the latest security patches
B. Application testing was completed by system administrators
C. Poor network performance was reported during recovery
D. Some restored systems were not listed in the DNS table of the DR subnet

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 346

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

A. detect potential fraud
B. prevent unauthorized changes to networks
C. comply with corporate policies
D. detect threats across environments

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 347

Which of the following is MOST difficult to achieve in a public cloud-computing environment?

A. Cost reduction
B. Pay per use
C. On-demand provisioning
D. Ability to audit

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 348

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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 349
When training an incident response team, the advantage of using tabletop exercises is that they:

A. provide the team with practical experience in responding to incidents
B. ensure that the team can respond to any incident
C. remove the need to involve senior managers in the response process
D. enable the team to develop effective response interactions

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 350
An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resource to support clients. The BEST approach to obtain the support of business unit management would be to:

A. present an analysis of the cost and benefit of the changes
B. discuss the risk and impact of security incidents if not implemented
C. present industry benchmarking results to business units
D. elaborate on the positive impact to information security

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE

Explanation

Explanation/Reference:

QUESTION 351

Ensuring that an organization can conduct security reviews within third-party facilities is PRIMARILY enabled by:

A. service level agreements (SLAs)
B. acceptance of the organization's security policies
C. contractual agreements
D. audit guidelines

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 352

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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 353

Which of the following will protect the confidentiality of data transmitted over the Internet?

A. Message digests
B. Network address translation
C. Encrypting file system
D. IPsec protocol

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 354

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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 355

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: INCIDENT MANAGEMENT AND RESPONSE
QUESTION 356

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

A. document and report the root cause of the incidents for senior management.
B. identify security program gaps or systemic weaknesses that need correction.
C. prepare properly vetted notifications regarding the incidents to external parties.

Explanation

Explanation/Reference:
D. identify who should be held accountable for the security incidents.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 357
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 358
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 359
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 360
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: INCIDENT MANAGEMENT AND RESPONSE
QUESTION 361
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

Explanation

Explanation/Reference:

QUESTION 362

After detecting an advanced persistent threat (APT), which of the following should be the information security manager's FIRST step?

A. Notify management
B. Contain the threat
C. Remove the threat
D. Perform root-cause analysis

Correct Answer: A

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 363

A newly hired information security manager reviewing an existing security investment plan is MOST likely to be concerned when the plan:

A. is based solely on a review of security threats and vulnerabilities in existing IT systems
B. identifies potential impacts that the implementation may have on business processes
C. focuses on compliance with common international security standards
D. has summarized IT costs for implementation rather than providing detail

Correct Answer: A

Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 364

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

A. Business impact if threats materialize
B. Availability of unused funds in the security budget
C. Threat information from reputable sources
D. Alignment of the new initiative with the approved business strategy

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 365
Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

A. An intrusion detection system
B. Established security baselines
C. Penetration testing

D. Log aggregation and correlation

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 366
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 367
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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:
QUESTION 368

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: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 369
Which of the following is the MOST appropriate board-level activity for information security governance?

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference:

QUESTION 370
Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

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

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE Explanation

Explanation/Reference: