CISM.isaca

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

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
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 2
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 3
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 4
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 5
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 6
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 7
The MOST important function of a risk management program is to:

A. quantify overall risk.
B. minimize residual risk.
C. eliminate inherent risk.
D. maximize the sum of all annualized loss expectancies (ALEs).

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred; this is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

QUESTION 8
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

A. Theft of purchased software
B. Power outage lasting 24 hours
C. Permanent decline in customer confidence
D. Temporary loss of e-mail due to a virus attack

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

QUESTION 9

Which of the following will BEST prevent external security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Securing and analyzing system access logs

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

QUESTION 10

In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

A. original cost to acquire.
B. cost of the software stored.
C. annualized loss expectancy (ALE).

D. cost to obtain a replacement.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
The value of the server should be based on its cost of replacement. The original cost may be significantly different from the current cost and, therefore, not as relevant. The value of the software is not at issue because it can be restored from backup media. The ALE for all risks related to the server does not represent the server's value.

QUESTION 11
A business impact analysis (BIA) is the BEST tool for calculating:

A. total cost of ownership.
B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A business impact analysis (BIA) is the best tool for calculating the priority of restoration for applications. It is not used to determine total cost of ownership, annualized loss expectancy (ALE) or residual risk to the organization.

QUESTION 12
When residual risk is minimized:

A. acceptable risk is probable.
B. transferred risk is acceptable.
C. control risk is reduced.
D. risk is transferable.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

QUESTION 13
Quantitative risk analysis is MOST appropriate when assessment data:

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 14
Which of the following is the MOST appropriate use of gap analysis?

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

Correct Answer: D

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 15
Identification and prioritization of business risk enables project managers to:
A. establish implementation milestones.
B. reduce the overall amount of slack time.
C. address areas with most significance.
D. accelerate completion of critical paths.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 16
A risk analysis should:

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 17
The recovery point objective (RPO) requires which of the following?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 18
Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 19
Which of the following BEST describes the scope of risk analysis?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 20
The decision as to whether a risk has been reduced to an acceptable level should be determined by:

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 21
Which of the following is the PRIMARY reason for implementing a risk management program?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 22
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

A. External auditors
B. A peer group within a similar businessC. Process owners
D. A specialized management consultant

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 23
A successful risk management program should lead to:

A. optimization of risk reduction efforts against cost.

B. containment of losses to an annual budgeted amount.
C. identification and removal of all man-made threats.
D. elimination or transference of all organizational risks.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 24
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
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 57
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 58
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 59
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 60
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 61
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 62
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 63
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 64
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 65
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 66
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 67
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 68
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 69
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 70
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 71
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 it's 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 72
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 73
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 74
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 75
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 76
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 77
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 78
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 79
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 80
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 81
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 82
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 83
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 84
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 85
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 86
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 87
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 88
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 89
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 90
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 91
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 92
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 93
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 94
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 95

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 96

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 97

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

A. Business impact analysis (BIA)
B. Penetration testing
C. Audit and review
D. Threat analysis

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Penetration testing focuses on identifying vulnerabilities. None of the other choices would identify vulnerabilities introduced by changes.

QUESTION 98

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

A. Countermeasure cost-benefit analysis
B. Penetration testing
C. Frequent risk assessment programs
D. Annual loss expectancy (ALE) calculation

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control. Frequent risk assessment

programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will contribute to the value of the risk but. alone, will not justify a control.

QUESTION 99
An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:
A. eliminating the risk.
B. transferring the risk.
C. mitigating the risk.D. accepting the risk.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

QUESTION 100
Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

A. Manager
B. Custodian
C. User
D. Owner

Correct Answer: D

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Although the information owner may be in a management position and is also considered a user, the information owner role has the responsibility for determining information classification levels. Management is responsible for higher-level issues such as providing and approving budget, supporting activities, etc. The information custodian is responsible for day-to-day security tasks such as protecting information, backing up information, etc. Users are the lowest level. They use the data, but do not classify the data. The owner classifies the data.

QUESTION 101
The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

A. determining the scope for inclusion in an information security program.
B. defining the level of access controls.
C. justifying costs for information resources.
D. determining the overall budget of an information security program.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The assigned class of sensitivity and criticality of the information resource determines the level of access controls to be put in place. The assignment of sensitivity and criticality takes place with the information assets that have already been included in the information security program and has only an indirect bearing on the costs to be incurred. The assignment of sensitivity and criticality contributes to, but does not decide, the overall budget of the information security program.

QUESTION 102
An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

A. Key performance indicators (KPIs)
B. Business impact analysis (BIA)
C. Gap analysis
D. Technical vulnerability assessment

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Gap analysis would help identify the actual gaps between the desired state and the current implementation of information security management. BIA is primarily used for business continuity planning. Technical vulnerability assessment is used for detailed assessment of technical controls, which would come later in the process and would not provide complete information in order to identify gaps.

QUESTION 103
When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

A. Estimated productivity losses
B. Possible scenarios with threats and impacts
C. Value of information assets
D. Vulnerability assessment

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

QUESTION 104
Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

A. User assessments of changes
B. Comparison of the program results with industry standards
C. Assignment of risk within the organization
D. Participation by all members of the organization

Correct Answer: D

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Effective risk management requires participation, support and acceptance by all applicable members of the organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

QUESTION 105
The MOST effective use of a risk register is to:
A. identify risks and assign roles and responsibilities for mitigation.
B. identify threats and probabilities.
C. facilitate a thorough review of all IT-related risks on a periodic basis.
D. record the annualized financial amount of expected losses due to risks.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A risk register is more than a simple list — it should lie used as a tool to ensure comprehensive documentation, periodic review and formal update of all risk elements in the enterprise's IT and related organization. Identifying risks and assigning roles and responsibilities for mitigation are elements of the register. Identifying threats and probabilities are two elements that are defined in the risk matrix, as differentiated from the broader scope of content in, and purpose for, the risk register. While the annualized loss expectancy (ALE) should be included in the register, this quantification is only a single element in the overall risk analysis program.

QUESTION 106
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

A. Define security metrics
B. Conduct a risk assessment
C. Perform a gap analysis
D. Procure security tools

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

When establishing an information security program, conducting a risk assessment is key to identifying the needs of the organization and developing a security strategy. Defining security metrics, performing a gap analysis and procuring security tools are all subsequent considerations.

QUESTION 107
Which of the following are the essential ingredients of a business impact analysis (B1A)?
A. Downtime tolerance, resources and criticality
B. Cost of business outages in a year as a factor of the security budget
C. Business continuity testing methodology being deployed
D. Structure of the crisis management team

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function. Options B, C and D are all associated with business continuity planning, but are not related to the BIA.

QUESTION 108
A risk management approach to information protection is:

A. managing risks to an acceptable level, commensurate with goals and objectives.
B. accepting the security posture provided by commercial security products.
C. implementing a training program to educate individuals on information protection and risks.
D. managing risk tools to ensure that they assess all information protection vulnerabilities.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk management is identifying all risks within an organization, establishing an acceptable level of risk and effectively managing risks which may include mitigation or transfer. Accepting the security- posture provided by commercial security products is an approach that would be limited to technology components and may not address all business operations of the organization. Education is a part of the overall risk management process. Tools may be limited to technology and would not address non-technology risks.

QUESTION 109
Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

A. Implement countermeasures.

B. Eliminate the risk.
C. Transfer the risk.
D. Accept the risk.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risks are typically transferred to insurance companies when the probability of an incident is low but the impact is high. Examples include: hurricanes, tornados and earthquakes. Implementing countermeasures may not be the most cost-effective approach to security management. Eliminating the risk may not be possible. Accepting the risk would leave the organization vulnerable to a catastrophic disaster which may cripple or ruin the organization. It would be more cost effective to pay recurring insurance costs than to be affected by a disaster from which the organization cannot financially recover.

QUESTION 110
To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

A. Conducting a qualitative and quantitative risk analysis.
B. Assigning value to the assets.
C. Weighing the cost of implementing the plan vs. financial loss.
D. Conducting a business impact analysis (BIA).

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

BIA is an essential component of an organization's business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. It is the first crucial step in business continuity planning. Qualitative and quantitative risk analysis will have been completed to define the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. Assigning value to assets is part of the BIA process. Weighing the cost of implementing the plan vs. financial loss is another part of the BIA.

QUESTION 111
An information security organization should PRIMARILY:

A. support the business objectives of the company by providing security-related support services.
B. be responsible for setting up and documenting the information security responsibilities of the information security team members.
C. ensure that the information security policies of the company are in line with global best practices and standards.
D. ensure that the information security expectations are conveyed to employees.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The information security organization is responsible for options B and D within an organization, but they are not its primary mission. Reviewing and adopting appropriate standards (option C) is a requirement. The primary objective of an information security organization is to ensure that security supports the overall business objectives of the company.

QUESTION 112
When implementing security controls, an information security manager must PRIMARILY focus on:

A. minimizing operational impacts.
B. eliminating all vulnerabilities.
C. usage by similar organizations.
D. certification from a third party.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security controls must be compatible with business needs. It is not feasible to eliminate all vulnerabilities. Usage by similar organizations does not guarantee that controls are adequate. Certification by a third party is important, but not a primary concern.

QUESTION 113
All risk management activities are PRIMARILY designed to reduce impacts to:

A. a level defined by the security manager.
B. an acceptable level based on organizational risk tolerance.
C. a minimum level consistent with regulatory requirements.
D. the minimum level possible.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The aim of risk management is to reduce impacts to an acceptable level. "Acceptable" or "reasonable" are relative terms that can vary based on environment and circumstances. A minimum level that is consistent with regulatory requirements may not be consistent with business objectives, and regulators typically do not assign risk levels. The minimum level possible may not be aligned with business requirements.

QUESTION 114
After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

A. Information security officer
B. Chief information officer (CIO)
C. Business owner
D. Chief executive officer (CFO)

Correct Answer: C

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The business owner of the application needs to understand and accept the residual application risks.

QUESTION 115
The purpose of a corrective control is to:

A. reduce adverse events.
B. indicate compromise.
C. mitigate impact.
D. ensure compliance.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Corrective controls serve to reduce or mitigate impacts, such as providing recovery capabilities. Preventive controls reduce adverse events, such as firewalls. Compromise can be detected by detective controls, such as intrusion detection systems (IDSs). Compliance could be ensured by preventive controls, such as access controls.

QUESTION 116
Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

A. Performing a business impact analysis (BIA)
B. Considering personal information devices as pan of the security policy
C. Initiating IT security training and familiarization
D. Basing the information security infrastructure on risk assessment

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The information security infrastructure should be based on risk. While considering personal information devices as part of the security policy may be a consideration, it is not the most important requirement. A BIA is typically carried out to prioritize business processes as part of a business continuity plan. Initiating IT security training may not be important for the purpose of the information security infrastructure.

QUESTION 117
Previously accepted risk should be:

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 118

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

A. perform a comprehensive assessment of the organization's exposure to the hacker's techniques.
B. initiate awareness training to counter social engineering.
C. immediately advise senior management of the elevated risk.
D. increase monitoring activities to provide early detection of intrusion.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 119
Which of the following steps should be performed FIRST in the risk assessment process?

A. Staff interviews

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk.

Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

QUESTION 120
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism
C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 121
An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?
A. Nothing, since a risk assessment was completed during development.
B. A vulnerability assessment should be conducted.
C. A new risk assessment should be performed.
D. The new vendor's SAS 70 type II report should be reviewed.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 122
Who can BEST advocate the development of and ensure the success of an information security program?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 123
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 124
The effectiveness of virus detection software is MOST dependent on which of the following?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 125
Which of the following is the MOST effective type of access control?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 126
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 127
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 128
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 129
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 130
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 131
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 132
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 133
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 134
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 135
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 136
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 137
Which of the following is MOST effective in preventing security weaknesses in operating systems?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 138
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 139
Who can BEST approve plans to implement an information security governance framework?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 140
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 141
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 authentication
D. Embedded digital signature

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 142

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 143

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 144
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 145
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 146
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 147
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.

A.

QUESTION 148

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

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 149

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

A.
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 150
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?
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 151
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

A.

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 152
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 153
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 154
Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

C.

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 155
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 156
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

A. SWOT analysis

B. Waterfall chart
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 157
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 158
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?

C.

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 159
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 160
Which of the following is MOST important for a successful information security program?

C.

A. Adequate training on emerging security technologies
B. Open communication with key process owners
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 161
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 162
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 163
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

C.

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 164
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 165
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 166

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 167

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 168
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 169
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 170
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

A. Authentication
B. Hardening
C. Encryption
D. Nonrepudiation

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 171
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 172
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 173
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 174
Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 175
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 176

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

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 177
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 178
Which of the following is MOST effective in protecting against the attack technique known as phishing?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

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

QUESTION 179
When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 180
Which of the following is the MOST important risk associated with middleware in a client-server environment?

A. Server patching may be prevented
B. System backups may be incomplete

C. System integrity may be affected
D. End-user sessions may be hijacked

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 181
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

A. Security in storage and transmission of sensitive data
B. Provider's level of compliance with industry standards
C. Security technologies in place at the facility
D. Results of the latest independent security review

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 182
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

A. Configuration of firewalls

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 183
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 184
The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 185
An information security manager uses security metrics to measure the:

A. performance of the information security program.
B. performance of the security baseline.
C. effectiveness of the security risk analysis.

D. effectiveness of the incident response team.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 186
The MOST important success factor to design an effective IT security awareness program is to:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 187
Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

A. Use security tokens for authentication
B. Connect through an IPSec VPN
C. Use https with a server-side certificate

D. Enforce static media access control (MAC) addresses

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 188
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

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

D. Multiple encryption algorithms

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 189
The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 190
A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:
A.

B.

authentication and authorization.
confidentiality and integrity.

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 191
When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 192
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

B.

C.

A. Security compliant servers trend report Percentage
of security compliant servers
Number of security patches applied
D. Security patches applied trend report

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 193
It is important to develop an information security baseline because it helps to define:

A. critical information resources needing protection.
B. a security policy for the entire organization.
C. the minimum acceptable security to be implemented.
D. required physical and logical access controls.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 194
Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

C.

D.

A. Symmetric cryptography
B. Public key infrastructure (PKI)
Message hashing

D.

E.

Message authentication code

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 195
Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 196
To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A. revise the information security program.

B. evaluate a balanced business scorecard.
C. conduct regular user awareness sessions.
D. perform penetration tests.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 197
What is the MOST important item to be included in an information security policy?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 198
In an organization, information systems security is the responsibility of:

A. all personnel.

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 199
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. invite an external consultant to create the security strategy.
B. allocate budget based on best practices.
C. benchmark similar organizations.
D. define high-level business security requirements.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 200
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

A. Number of controls

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 201
Which of the following would be the BEST metric for the IT risk management process?

A. Number of risk management action plans
B. Percentage of critical assets with budgeted remedial
C. Percentage of unresolved risk exposures
D. Number of security incidents identified

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 202
Which of the following is a key area of the ISO 27001 framework?

A. Operational risk assessment
B. Financial crime metrics

C. Capacity management
D. Business continuity management

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 203
The MAIN goal of an information security strategic plan is to:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 204
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 205
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the system.
B. implement multifactor authentication.
C. rebuild the system from the original installation medium.
D. disconnect the mail server from the network.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 206
The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

A.

verify the decision with the business units.

B. check the system's risk analysis.
C. recommend update after post implementation review.
D. request an audit review.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 207
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks
B. Traffic sniffing
C. Virus infections
D. IP address spoofing

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 208
The PRIMARY objective of an Internet usage policy is to prevent:

B.

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 209
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 210
A test plan to validate the security controls of a new system should be developed during which phase of the project?

C.

A. Testing
B. Initiation
Design
D. Development

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 211
The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 212
In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

D.

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

E.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 213
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 214
Priority should be given to which of the following to ensure effective implementation of information security governance?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 215
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 216
Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

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

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 217
Which of the following is the MOST important reason why information security objectives should be defined?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 218
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A. Authentication
B. Encryption
C. Prohibit employees from copying data to USB devices
D. Limit the use of USB devices

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

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

QUESTION 219
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 220
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

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

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 221
What is the MOST important reason for conducting security awareness programs throughout an organization?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 222
At what stage of the applications development process would encryption key management initially be addressed?

A. Requirements development
B. Deployment
C. Systems testing
D. Code reviews

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

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

QUESTION 223
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet web site does not force users to access it and read the information. Circulating the information security policy atone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

QUESTION 224
Which of the following would be the BEST defense against sniffing?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 225
A digital signature using a public key infrastructure (PKI) will:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 226
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

A. to u higher false reject rate (FRR).
B. to a lower crossover error rate.
C. to a higher false acceptance rate (FAR).
D. exactly to the crossover error rate.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

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

QUESTION 227
Which of the following is the BEST method to securely transfer a message?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 228
Which of the following would be the FIRST step in establishing an information security program?

A. Develop the security policy.
B. Develop security operating procedures.
C. Develop the security plan.
D. Conduct a security controls study.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A security plan must be developed to implement the security strategy. All of the other choices should follow the development of the security plan.

QUESTION 229
An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross training. Which type of authorization policy would BEST address this practice?

A. Multilevel
B. Role-based
C. Discretionary
D. Attribute-based

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A role-based policy will associate data access with the role performed by an individual, thus restricting access to data required to perform the individual's tasks. Multilevel policies are based on classifications and clearances. Discretionary policies leave access decisions up to information resource managers.

QUESTION 230
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

A. the parties to the agreement can perform.
B. confidential data are not included in the agreement.
C. appropriate controls are included.
D. the right to audit is a requirement.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Agreements with external parties can expose an organization to information security risks that must be assessed and appropriately mitigated. The ability of the parties to perform is normally the responsibility of legal and the business operation involved. Confidential information may be in the agreement by necessity and. while the information security manager can advise and provide approaches to protect the information, the responsibility rests with the business and legal. Audit rights may be one of many possible controls to include in a third-party agreement, but is not necessarily a contract requirement, depending on the nature of the agreement.

QUESTION 231
For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

A. Biometrics
B. Symmetric encryption keys
C. Secure Sockets Layer (SSL)-based authentication
D. Two-factor authentication

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

QUESTION 232
Which of the following guarantees that data in a file have not changed?

A. Inspecting the modified date of the file
B. Encrypting the file with symmetric encryption
C. Using stringent access control to prevent unauthorized access
D. Creating a hash of the file, then comparing the file hashes

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:
A hashing algorithm can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

QUESTION 233
Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

A. Filter media access control (MAC) addresses
B. Use a Wi-Fi Protected Access (WPA2) protocol
C. Use a Wired Equivalent Privacy (WEP) key
D. Web-based authentication

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

WPA2 is currently one of the most secure authentication and encryption protocols for mainstream wireless products. MAC address filtering by itself is not a good security mechanism since allowed MAC addresses can be easily sniffed and then spoofed to get into the network. WEP is no longer a secure encryption mechanism for wireless communications. The WEP key can be easily broken within minutes using widely available software. And once the WEP key is obtained, all communications of every other wireless client are exposed. Finally, a web-based authentication mechanism can be used to prevent unauthorized user access to a network, but it will not solve the wireless network's main security issues, such as preventing network sniffing.

QUESTION 234
Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

A. An intrusion prevention system (IPS)
B. An intrusion detection system (IDS)
C. A host-based intrusion detection system (HIDS)
D. A host-based firewall

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect, but not prevent I IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

QUESTION 235
Nonrepudiation can BEST be ensured by using:

A. strong passwords.
B. a digital hash.
C. symmetric encryption.
D. digital signatures.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Digital signatures use a private and public key pair, authenticating both parties. The integrity of the contents exchanged is controlled through the hashing mechanism that is signed by the private key of the exchanging party. A digital hash in itself helps in ensuring integrity of the contents, but not nonrepudiation. Symmetric encryption wouldn't help in nonrepudiation since the keys are always shared between parties. Strong passwords only ensure authentication to the system and cannot be used for nonrepudiation involving two or more parties.

QUESTION 236
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 237
A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 238
The BEST way to ensure that information security policies are followed is to:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 239
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 240
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 241
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 242
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 243
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 244
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 245
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 246
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 247
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 248
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 249
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 250
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 251
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 252
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 253
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 254
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 255
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 256
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 257
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 258
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 259
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 260
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 261
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 262
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 263
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 264
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 265
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 266
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 267
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 268
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 269
Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

A. assess the problems and institute rollback procedures, if needed.
B. disconnect the systems from the network until the problems are corrected.
C. immediately uninstall the patches from these systems.
D. immediately contact the vendor regarding the problems that occurred.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Assessing the problems and instituting rollback procedures as needed would be the best course of action. Choices B and C would not identify where the problem was, and may in fact make the problem worse. Choice D is part of the assessment.

QUESTION 270
When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

A. access control matrix.
B. encryption strength.
C. authentication mechanism.
D. data repository.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The access control matrix is the best indicator of the level of compliance with the service level agreement (SLA) data confidentiality clauses. Encryption strength, authentication mechanism and data repository might be defined in the SLA but are not confidentiality compliance indicators.

QUESTION 271
The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

A. identifying vulnerabilities in the system.
B. sustaining the organization's security posture.
C. the existing systems that will be affected.
D. complying with segregation of duties.

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is important to maintain the organization's security posture at all times. The focus should not be confined to the new system being developed or acquired, or to the existing systems in use. Segregation of duties is only part of a solution to improving the security of the systems, not the primary reason to involve security in the systems development life cycle (SDLC).

QUESTION 272
The implementation of continuous monitoring controls is the BEST option where:
A. incidents may have a high impact and frequency
B. legislation requires strong information security controls
C. incidents may have a high impact but low frequency
D. Electronic commerce is a primary business driver

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Continuous monitoring control initiatives are expensive, so they have to be used in areas where the risk is at its greatest level. These areas are the ones with high impact and high frequency of occurrence. Regulations and legislations that require tight IT security measures focus on requiring organizations to establish an IT security governance structure that manages IT security with a risk-based approach, so each organization decides which kinds of controls are implemented. Continuous monitoring is not necessarily a requirement. Measures such as contingency planning are commonly used when incidents rarely happen but have a high impact each time they happen. Continuous monitoring is unlikely to be necessary. Continuous control monitoring initiatives are not needed in all electronic commerce environments. There are some electronic commerce environments where the impact of incidents is not high enough to support the implementation of this kind of initiative.

QUESTION 273
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

A. System monitoring for traffic on network ports
B. Security code reviews for the entire application

C. Reverse engineering the application binaries
D. Running the application from a high-privileged account on a test system

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Security' code reviews for the entire application is the best measure and will involve reviewing the entire source code to detect all instances of back doors. System monitoring for traffic on network ports would not be able to detect all instances of back doors and is time consuming and would take a lot of effort. Reverse engineering the application binaries may not provide any definite clues. Back doors will not surface by running the application on high-privileged accounts since back doors are usually hidden accounts in the applications.

QUESTION 274
An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

A. source routing.
B. broadcast propagation.
C. unregistered ports.
D. nonstandard protocols.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

If the firewall allows source routing, any outsider can carry out spoofing attacks by stealing the internal (private) IP addresses of the organization. Broadcast propagation, unregistered ports and nonstandard protocols do not create a significant security exposure.

QUESTION 275
What is the MOS T cost-effective means of improving security awareness of staff personnel?

A. Employee monetary incentives
B. User education and training
C. A zero-tolerance security policy

D. Reporting of security infractions

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

User education and training is the most cost-effective means of influencing staff to improve security since personnel are the weakest link in security. Incentives perform poorly without user education and training. A zero-tolerance security policy would not be as good as education and training. Users would not have the knowledge to accurately interpret and report violations without user education and training.

QUESTION 276
Which of the following is the MOST effective at preventing an unauthorized individual from following an authorized person through a secured entrance (tailgating or piggybacking)?

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

Correct Answer: D
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. The other choices are physical controls which by themselves would not be effective against tailgating.

QUESTION 277
Data owners will determine what access and authorizations users will have by:

A. delegating authority to data custodian.
B. cloning existing user accounts.
C. determining hierarchical preferences.

D. mapping to business needs.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Access and authorizations should be based on business needs. Data custodians implement the decisions made by data owners. Access and authorizations are not to be assigned by cloning existing user accounts or determining hierarchical preferences. By cloning, users may obtain more access rights and privileges than is required to do their job. Hierarchical preferences may be based on individual preferences and not on business needs.

QUESTION 278
Which of the following is the MOST likely outcome of a well-designed information security awareness course?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 279
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

All new employees will need to understand techniques for the construction of strong passwords. The other choices would not be applicable to general staff employees.

QUESTION 280
A critical component of a continuous improvement program for information security is:

A. measuring processes and providing feedback.
B. developing a service level agreement (SLA) for security.
C. tying corporate security standards to a recognized international standard.
D. ensuring regulatory compliance.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 281
The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 282
An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

troublesome in large organizations. In discretionary access control, users have access to resources based on predefined sets of principles, which is an inherently insecure approach.

QUESTION 283
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is critical to include the security requirements in the contract based ON the company's security policy to ensure that the necessary security controls are implemented by the service provider. The audit is normally a one-time effort and cannot provide ongoing assurance of the security. A nondisclosure agreement (NDA) should be part of the contract; however, it is not critical to the security of the web site. Penetration testing alone would not provide total security to the web site; there are lots of controls that cannot be tested through penetration testing.

QUESTION 284
Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 285
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 286
An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 287
Which of the following would raise security awareness among an organization's employees?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 288
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?
A. Attempt to reset several passwords to weaker values
B. Install code to capture passwords for periodic audit
C. Sample a subset of users and request their passwords for review
D. Review general security settings on each platform

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 289
What is the MOST cost-effective method of identifying new vendor vulnerabilities?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 290
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audits.

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Defining and monitoring security metrics is a good approach to analyze the performance of the security management process since it determines the baseline and evaluates the performance against the baseline to identify an opportunity for improvement. This is a systematic and structured approach to process improvement. Audits will identify deficiencies in established controls; however, they are not effective in evaluating the overall performance for improvement. Penetration testing

will only uncover technical vulnerabilities, and cannot provide a holistic picture of information security management, feedback is subjective and not necessarily reflective of true performance.

QUESTION 291
An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 292
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:
A. uses multiple redirects for completing a data commit transaction.
B. has implemented cookies as the sole authentication mechanism.
C. has been installed with a non-legitimate license key.
D. is hosted on a server along with other applications.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 293
Of the following, retention of business records should be PRIMARILY based on:

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 294
An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 295
An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 296
Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

A. Provide security awareness training to the third-party provider's employees
B. Conduct regular security reviews of the third-party provider
C. Include security requirements in the service contract
D. Request that the third-party provider comply with the organization's information security policy

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 297
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 298
Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

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

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 299
Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 300
In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

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

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 301
Which of the following is generally considered a fundamental component of an information security program?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 302
How would an organization know if its new information security program is accomplishing its goals?
A. Key metrics indicate a reduction in incident impacts.
B. Senior management has approved the program and is supportive of it.
C. Employees are receptive to changes that were implemented.
D. There is an immediate reduction in reported incidents.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 303
A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 304
Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A. Acceptable use policy

B. Setting low mailbox limitsC. User awareness training
D. Taking disciplinary action

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 305
Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 306
Which of the following measures is the MOST effective deterrent against disgruntled stall abusing their privileges?

A. Layered defense strategy
B. System audit log monitoring

C. Signed acceptable use policy
D. High-availability systems

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 307
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 308
As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A. considered at the discretion of the information owner.

B. approved by the next higher person in the organizational structure.
C. formally managed within the information security framework.
D. reviewed and approved by the security manager.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 309
There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

A. Black box pen test
B. Security audit
C. Source code review
D. Vulnerability scan

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Source code review is the best way to find and remove an application backdoor. Application backdoors can be almost impossible to identify' using a black box pen test or a security audit. A vulnerability scan will only find "known" vulnerability patterns and will therefore not find a programmer's application backdoor.

QUESTION 310
Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does il always introduce?

A. Remote buffer overflow

B. Cross site scripting
C. Clear text authentication
D. Man-in-the-middle attack

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

One of the main problems with using SNMP vl and v°2 is the clear text "community string" that it uses to authenticate. It is easy to sniff and reuse. Most times, the SNMP community string is shared throughout the organization's servers and routers, making this authentication problem a serious threat to security. There have been some isolated cases of remote buffer overflows against SNMP daemons, but generally that is not a problem. Cross site scripting is a web application vulnerability that is not related to SNMP. A man-in-the-middle attack against a user datagram protocol (UDP) makes no sense since there is no active session; every request has the community string and is answered independently.

QUESTION 311
Which of the following is the FIRST phase in which security should be addressed in the development cycle of a project?

A. Design
B. Implementation
C. Application security testing
D. Feasibility

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information security should be considered at the earliest possible stage. Security requirements must be defined before you enter into design specification, although changes in design may alter these requirements later on. Security requirements defined during system implementation are typically costly add-ons that are frequently ineffective. Application security testing occurs after security has been implemented.

QUESTION 312

B.
Which of the following should be determined FIRST when establishing a business continuity program?

A. Cost to rebuild information processing facilities
Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION 313
A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. disconnecting the computer from all power sources.
B. disabling all local user accounts except for one administrator.
C. encrypting local files and uploading exact copies to a secure server.
D. copying all files using the operating system (OS) to write-once media.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing it remotely changes the operating system (OS) and temporary files on the computer and invalidates it as admissible evidence.

B.

QUESTION 314

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 315

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:

B.
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 316
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.

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 honcypots, 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 317
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

B.

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 318

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 319
Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot site?

A. Tests are scheduled on weekends
B. 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 320
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 321
An incident response policy must contain:

A. updated call trees.
B. escalation criteria.
C. 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 322
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 323
A post-incident review should be conducted by an incident management team to determine:

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

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 324
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.