VCEplus
VCE To PDF - Free Practice Exam

ISACA_CertifyMe_CISM_v2011-04-21_304q_By-Simon

Number: CISM
Passing Score: 800
Time Limit: 120 min
File Version: 2011-04-21

VCEplus
VCE To PDF - Free Practice Exam

Exam Name = ISACA

Exam Code = CISM

Version = 2011-04-21

The Whole Study Material is hundred percent valid..

Good Luck Guys

By = Simon

VCEplus
VCE To PDF - Free Practice Exam

Exam A

QUESTION 1
Senior management commitment and support for information security can BEST be obtained through presentations that:

A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best security practices.
D. tie security risks to key business objectives.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they are presented in terms of key business objectives.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 2
Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economies of scale. However, turnaround can be slower due to the lack of alignment with business units.

QUESTION 3
The MOST important component of a privacy policy is:

A. notifications
B. warranties
C. liabilities
D. geographic coverage

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Privacy policies must contain notifications and opt-out provisions; they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

QUESTION 4
It is MOST important that information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices is secondary by comparison.

QUESTION 5
Security technologies should be selected PRIMARILY on the basis of their:

A. ability to mitigate business risks
B. evaluations in trade publications
C. use of new and emerging technologies
D. benefits in comparison to their costs

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The most fundamental evaluation criteria for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

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

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

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 7
The PRIMARY goal in developing an information security strategy is to:

A. establish security metrics and performance monitoring.
B. educate business process owners regarding their duties.
C. ensure that legal and regulatory requirements are met.
D. support the business objectives of the organization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

QUESTION 8
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

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

Correct Answer: A
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 9
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
B. establish baseline standards for all locations and add supplemental standards as required.
C. bring all locations into conformity with a generally accepted set of industry best practices.
D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a

lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach-forcing all locations to be in compliance with the regulations-places an undue burden on those locations.

QUESTION 10
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks
C. Demonstrate that IT mitigating controls are in place
D. Suggest new IT controls to mitigate operational risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The job of the information security officer on such a team is to assess the risks to the business operation. Choice A is incorrect because information security is not limited to IT issues. Choice C is incorrect because at the time a team is formed to assess risk, it is premature to assume that any demonstration of IT controls will mitigate business operations risk. Choice D is incorrect because it is premature at the time of the formation of the team to assume that any suggestion of new IT controls will mitigate business operational risk.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 11
From an information security manager perspective, what is the immediate benefit of clearly- defined roles and responsibilities?

A. Enhanced policy compliance
B. Improved procedure flows
C. Segregation of duties
D. Better accountability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Without well-defined roles and responsibilities, there cannot be accountability. Choice A is incorrect because policy compliance requires adequately defined accountability first and therefore is a byproduct. Choice B is incorrect because people can be assigned to execute procedures that are not well designed. Choice C is incorrect because segregation of duties is not automatic, and roles may still include conflicting duties.

QUESTION 12
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)
D. Return on security investment report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Performing a risk assessment will allow the information security manager to prioritize the remedial measures and provide a means to convey a sense of urgency to management. Metrics reports are normally contained within the methodology of the risk assessment to give it credibility and provide an ongoing tool. The business impact analysis (BIA) covers continuity risks only. Return on security investment cannot be determined until a plan is developed based on the BIA.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 13
Which of the following is responsible for legal and regulatory liability?

A. Chief security officer (CSO)
B. Chief legal counsel (CLC)
C. Board and senior management
D. Information security steering group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

QUESTION 14
Who in an organization has the responsibility for classifying information?

A. Data custodian

B. Database administrator
C. Information security officer
D. Data owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The data owner has full responsibility over data. The data custodian is responsible for securing the information. The database administrator carries out the technical administration. The information security officer oversees the overall classification management of the information.

QUESTION 15
Logging is an example of which type of defense against systems compromise?

A. Containment
B. Detection
C. Reaction
D. Recovery

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 16
Which of the following is MOST important in developing a security strategy?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 17
Which of the following factors is a primary driver for information security governance that does not require any further justification?

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

Correct Answer: D
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 18
A security manager meeting the requirements for the international flow of personal data will need to ensure:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 19
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

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

Correct Answer: B
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 20
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 21
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

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

Correct Answer: D
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 22
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 23
To achieve effective strategic alignment of security initiatives, it is important that:

A. steering committee leadershipbe selected by rotation.
B. inputs be obtained and consensus achieved between the major organizational units.
C. the business strategybe updated periodically.
D. procedures and standardsbe approved by all departmental heads.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 24
Which of the following will BEST protect an organization from internal security attacks?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 25
Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.

C. control risk is minimized.
D. inherent risk is minimized.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 26
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Residual risk provides management with sufficient information to decide on 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 27
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: (none)
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 28
A risk assessment should be conducted:

A. once a year for each business process andsubprocess.
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 29
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: (none)

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 30
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 31
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: (none)
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 32
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 33
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: (none)
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 34
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: (none)
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 35
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:

VCEplus
VCE To PDF - Free Practice Exam

A. thereare 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: (none)
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 36
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: (none)
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 37
Which of the following risks is represented in the risk appetite of an organization?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
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 38
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: (none)

VCEplus
VCE To PDF - Free Practice Exam

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 39
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 40
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: (none)
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 41
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: (none)
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 42
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 are network (LAN).
What should the security manager do FIRST?

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 43

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 (SSL) 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 44
Which of the following would BEST address the risk of data leakage?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: C
Section: (none)
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 45
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: (none)
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 46
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:

VCEplus
VCE To PDF - Free Practice Exam

A. broken authentication.

B. unvalidated input.

C. cross-site scripting.

D. Structured query language (SQL) injection.

Correct Answer: A
Section: (none)
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 47
When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

A. right-to-terminate clause.

VCEplus
VCE To PDF - Free Practice Exam

B. limitations of liability.
C. service level agreement (SLA).
D. financial penalties clause.

Correct Answer: C
Section: (none)
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 48
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
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 49
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: (none)
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 50
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 51
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

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

Correct Answer: D
Section: (none)
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 52
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 53
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: (none)
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 54
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 55
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: (none)
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 56
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 57
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: (none)
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 58
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: (none)
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 59
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?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: B
Section: (none)
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 60
Te MAIN goal of an information security strategic plan is to:

A. develop a risk assessment plan.

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: C
Section: (none)
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 a 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 61
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.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
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 62
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: (none)
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 63
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 64
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: (none)
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 65
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: (none)
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, but they do not address the issue of temporary employees as well as role-based access controls.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 66
Successful social engineering attacks can BEST be prevented through:

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

Correct Answer: C
Section: (none)
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 67

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 68
Which of the following is an inherent weakness of signature-based intrusion detection systems?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 69
Which of the following are the MOST important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer

B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal departments

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 70
Which of the following is the MOST important action to take when engaging third party consultants to conduct an attack and penetration test?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 71
Good information security standards should:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 72
Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

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

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 73
What is the MOST appropriate change management procedure for the handling of emergency program changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 74
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

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

Correct Answer: A
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 75
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 76
Which of the following events generally has the highest information security impact?

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

Correct Answer: B
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 77
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The research and development department is usually the most sensitive area of the pharmaceutical organization. Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical; therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

QUESTION 78
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

A. The program's governance oversight mechanisms
B. Information security periodicals and manuals
C. The program's security architecture and design
D. Training and certification of the information security team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While choices B, C and D will all assist the currency and coverage of the program, its governance oversight mechanisms are the best method.

QUESTION 79
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

A. Budget allocation
B. Technical skills of staff
C. User acceptance
D. Password requirements

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
End users may react differently to the implementation, and may have specific preferences. The information security manager should be aware that what is viewed as reasonable in one culture may not be acceptable in another culture. Budget allocation will have a lesser impact since what is rejected as a result of culture cannot be successfully implemented regardless of budgetary considerations. Technical skills of staff will have a lesser impact since new staff can be recruited or existing staff can be trained. Although important, password requirements would be less likely to guarantee the success of the implementation.

QUESTION 80
Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

A. Reconciliation of the annual systems inventory to the disaster recovery/business continuity plans

B. Periodic audits of the disaster recovery/business continuity plans
C. Comprehensive walk-through testing
D. Inclusion as a required step in the system life cycle process

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security should be an integral component of the development cycle; thus, it should be included at the process level. Choices A, B and C are good mechanisms to ensure compliance, but would not be nearly as timely in ensuring that the plans are always up-to-date. Choice D is a preventive control, while choices A, B and C are detective controls.

QUESTION 81
What is the GREATEST risk when there is an excessive number of firewall rules?

A. One rule may override another rule in the chain and create a loophole
B. Performance degradation of the whole network
C. The firewall may not support the increasing number of rules due to limitations
D. The firewall may show abnormal behavior and may crash or automatically shut down

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If there are many firewall rules, there is a chance that a particular rule may allow an external connection although other associated rules are overridden. Due to the increasing number of rules, it becomes complex to test them and, over time, a loophole may occur.

QUESTION 82
What is the BEST way to ensure data protection upon termination of employment?

A. Retrieve identification badge and card keys
B. Retrieve all personal computer equipment
C. Erase all of the employee's folders
D. Ensure all logical access is removed

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Ensuring all logical access is removed will guarantee that the former employee will not be able to access company data and that the employee's credentials will not be misused. Retrieving identification badge and card keys would only reduce the capability to enter the building. Retrieving the personal computer equipment and the employee's folders are necessary tasks, but that should be done as a second step.

QUESTION 83
Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

A. Conduct awareness sessions on intellectual property policy
B. Require all employees to sign a nondisclosure agreement
C. Promptly remove all access when an employee leaves the organization
D. Restrict access to a need-to-know basis

Correct Answer: D
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:
Explanation:
Security awareness regarding intellectual property policy will not prevent violations of this policy. Requiring all employees to sign a nondisclosure agreement and promptly removing all access when an employee leaves the organization are good controls, but not as effective as restricting access to a need-to-know basis.

QUESTION 84
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
D. Require that a change request be submitted for each download

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Administrative accounts have permission to change data. This is not required for the developers to perform their tasks. Unauthorized change will damage the integrity of the data. Logging all usage of the account, suspending the account and activating only when needed, and requiring that a change request be submitted for each download will not reduce the exposure created by this excessive level of access. Restricting the account to read only access will ensure that file integrity can be maintained while permitting access.

QUESTION 85
Which would be the BEST recommendation to protect against phishing attacks?

A. Install an anti spam system
B. Publish security guidance for customers
C. Provide security awareness to the organization's staff
D. Install an application-level firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Customers of the organization are the target of phishing attacks. Installing security software or training the organization's staff will be useless. The effort should be put on the customer side.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 86
What is the BEST way to alleviate security team understaffing while retaining the capability in- house?

A. Hire a contractor that would not be included in the permanent headcount
B. Outsource with a security services provider while retaining the control internally
C. Establish a virtual security team from competent employees across the company
D. Provide cross training to minimize the existing resources gap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While hiring an indirect resource that will not be part of headcount will help to add an extra resource, it usually costs more than a direct employee; thus, it is not cost efficient. Outsourcing may be a more expensive option and can add complexities to the service delivery. Competent security staff can be recruited from other departments- e.g., IT, product development, research and development (R&D). By leveraging existing resources, there is a nominal

additional cost. It is also a strategic option since the staff may join the team as full members in the future (internal transfer). Development of staff is often a budget drain and, if not managed carefully, these resources may move away from the company and leave the team with a bigger resource gap.

QUESTION 87
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 88
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: (none)
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 89
The FIRST priority when responding to a major security incident is:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 90
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 91
When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 92
When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 93
Which of the following provides the BEST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

A. The recovery time objective (RTO) was not exceeded during testing
B. Objective testing of the business continuity/disaster recovery plan has been carried out consistently
C. The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
D. Information assets have been valued and assigned to owners per the business continuity plan/disaster recovery plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Consistent achievement of recovery time objective (RTO) objectives during testing provides the most objective evidence that business continuity/ disaster recovery plan objectives have been achieved. The successful testing of the business continuity/disaster recovery plan within the stated RTO objectives is the most indicative evidence that the business needs are being met. Objective testing of the business continuity/disaster recovery plan will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning. Mere valuation and assignment of information assets to owners (per the business continuity/disaster recovery plan) will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning.

QUESTION 94
Which of the following situations would be the MOST concern to a security manager?

A. Audit logs are not enabled on a production server
B. The logon ID for a terminated systems analyst still exists on the system
C. The help desk has received numerous results of users receiving phishing e-mails
D. A Trojan was found to be installed on a system administrator's laptop

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The discovery of a Trojan installed on a system's administrator's laptop is highly significant since this may mean that privileged user accounts and passwords may have been compromised. The other choices, although important, do not pose as immediate or as critical a threat.

QUESTION 95
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the incident.
B. notify senior management.
C. start containment.
D. notify law enforcement.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Asserting that the condition is a true security incident is the necessary first step in determining the correct response. The containment stage would follow. Notifying senior management and law enforcement could be part of the incident response process that takes place after confirming an incident.

QUESTION 96
A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

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

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:
Explanation:

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

QUESTION 97
What is the BEST method for mitigating against network denial of service (DoS) attacks?

A. Ensure all servers are up-to-date on OS patches
B. Employ packet filtering to drop suspect packets
C. Implement network address translation to make internal addresses nonroutable
D. Implement load balancing for Internet facing devices

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Packet filtering techniques are the only ones which reduce network congestion caused by a network denial of service (DoS) attack. Patching servers,

in general, will not affect network traffic. Implementing network address translation and load balancing would not be as effective in mitigating most network DoS attacks.

QUESTION 98
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts
B. Write access violations
C. Concurrent logons
D. Firewall logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since the password for the shared administrative account was obtained through guessing, it is probable that there were multiple unsuccessful logon attempts before the correct password was deduced. Searching the logs for invalid logon attempts could, therefore, lead to the discovery of this unauthorized activity. Because the account is shared, reviewing the logs for concurrent logons would not reveal unauthorized activity since concurrent usage is common in this situation. Write access violations would not necessarily be observed since the information was merely copied and not altered. Firewall logs would not necessarily contain information regarding logon attempts.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 99
An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A warm site is not fully equipped with the company's main systems; therefore, the tapes should be tested using the company's production systems.

Inspecting the facility and checking the tape inventory does not guarantee that the tapes are usable.

QUESTION 100
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

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

Correct Answer: A
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 101
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 102
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

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

Correct Answer: D
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 103
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 104

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 105
In order to highlight to management the importance of network security, the security manager should FIRST:

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 106
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions

C. Organization chart
D. Skills inventory

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 107
The MOST important characteristic of good security policies is that they:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 108
An information security manager must understand the relationship between information security and business operations in order to:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 109
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 110
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

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

Correct Answer: C

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

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

QUESTION 111
Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

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

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 112
Which of the following is the MOST important element of an information security strategy?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 113
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

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

Correct Answer: C
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 114
Which of the following is the BEST justification to convince management to invest in an information security program?

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

Correct Answer: D
Section: (none)
Explanation

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

business assets.

QUESTION 115
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

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

Correct Answer: A
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 116
The MOST important factor in ensuring the success of an information security program, is effective:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 117

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

A. Key control monitoring
B. A robust security awareness program
C. A security program that enables business activities

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 118
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 119
The MOST complete business case for security solutions is one that:

A. includes appropriate justification.
B. explains the current risk profile.

VCEplus
VCE To PDF - Free Practice Exam

C. details regulatory requirements.
D. identifies incidents and losses.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 120
Which of the following is MOST important to understand when developing a meaningful information security strategy?

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 121
Which of the following is an advantage of a centralized information security organizational structure?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 122
Which of the following would help to change an organization's security culture?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
VCEplus
VCE To PDF - Free Practice Exam
Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditmg is not effective in changing the culture of the company.

QUESTION 123
The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 124
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 opportunitiesbe understood.

Correct Answer: C
Section: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 125
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: (none)
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 126
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: (none)
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 be considered a strategy.

QUESTION 127
Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 carry 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 128
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: (none)
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 129
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 incidents
C. Total cost of ownership (TCO)
D. Approved budget for the project

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
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 130
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: (none)
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 131
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
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 132
Who is responsible for ensuring that information is classified?

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

Correct Answer: C

Section: (none)
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 133
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:
Explanation:
When the cost of control is more than the cost of the risk, the nsk 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 134
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: (none)
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 135
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 136
Which of the 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: (none)
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 137
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: (none)
Explanation

Explanation/Reference:
Explanation:
Key controls primarily reduce risk and are most effective for the protection of information assets.
The other

QUESTION 138
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.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
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 139
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.

VCEplus
VCE To PDF - Free Practice Exam

D. identify privacy legislation in other countries that may contain similar requirements.

Correct Answer: B
Section: (none)
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 140
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.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
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 141
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: (none)
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 142
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: (none)
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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 143
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: (none)
Explanation

Explanation/Reference:

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

QUESTION 144
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 145
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: (none)
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 146
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: (none)
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 147
Priority should be given to which of the following to ensure effective implementation of information security governance?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 148
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: (none)
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 149
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 150
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: (none)
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 151
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 152
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: (none)
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- sawy 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 153
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 154
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: (none)
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 155
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: (none)
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 156
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 alone 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 157
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: (none)
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 ttaffic 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 158
A digital signature using a public key infrastructure (PKI) will:

VCEplus
VCE To PDF - Free Practice Exam

A. notensure 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: (none)
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 159
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

A. to a 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: (none)
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 160
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
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 161
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: (none)
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 162
An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage crosstraining. Which type of authorization policy would BEST address this practice?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 163
An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RFP) is the:

A. references from other organizations.
B. past experience of the engagement team.
C. sample deliverable.
D. methodology used in the assessment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Methodology illustrates the process and formulates the basis to align expectations and the execution of the assessment. This also provides a picture of what is required of all parties involved in the assessment. References from other organizations are important, but not as important as the methodology used in the assessment. Past experience of the engagement team is not as important as the methodology used. Sample deliverables only tell how the assessment is presented, not the process.

QUESTION 164
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. immediatelyuninstall the patches from these systems.
D. immediatelycontact the vendor regarding the problems that occurred.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VCEplus
VCE To PDF - Free Practice Exam

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 165
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: (none)
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 166
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: (none)
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).

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 167
The implementation of continuous monitoring controls is the BEST option where:

A. Incidents may have a high impact and frequency
B. Legislation requires strong in/orrnation security controls
C. Incidents may have a high impact but low frequency
D. Electronic commerce is a primary business driver

Correct Answer: A
Section: (none)
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. Regulation and legislations that requires 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 168
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 169
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: (none)
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 170

What is the MOST 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: (none)
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 171
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)?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: D
Section: (none)
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 172
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: (none)
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 cionmg 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 173
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
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 and 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 174
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

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

Correct Answer: B
Section: (none)
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 175
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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 176
The management staff of an organization that does not have a dedicated security function decide 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: (none)
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 177
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 178
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: (none)
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 179
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: (none)
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.

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 180
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: (none)
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 181

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 182
Which of the following would raise security awareness among an organization's employees?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: D
Section: (none)
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 183
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: (none)
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 184
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
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. Honey pots would not identify all vendor vulnerabilities. In addition, honey pots located in the DMZ can create a security risk if the production network is not well protected from traffic from compromised honey pots.

QUESTION 185
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: (none)
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 186
When developing metrics to measure and monitor information security programs, the information security manager should ensure that the metrics reflect the:

A. residual risks.
B. levels of security.
C. security objectives.
D. statistics of security incidents.

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:
Explanation:
Metrics should be developed based on security objectives, so they it can measure the effectiveness and efficiency of information security controls. Metrics are not only used to measure the results of the security controls (residual risks), but also the attributes of the control implementation. Metrics are not only used to measure the result of the security controls (levels of security), but also the attributes of the control implementation. Not only statistics are collected, but other attributes of the information security controls should also be considered.

QUESTION 187
An organization has learned of a Security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

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

Correct Answer: A

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

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

QUESTION 188
Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

A. Communicating specially drafted messages by an authorized person
B. Refusing to comment until recovery
C. Referring the media to the authorities
D. Reporting the losses and recovery strategy to the media

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

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

QUESTION 189
During the security review of organizational servers it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the security manager should:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 190
If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A. obtaining evidence as soon as possible.
B. preserving the integrity of the evidence.
C. disconnecting all IT equipment involved.
D. reconstructing the sequence of events.

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:
Explanation:
The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are part of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

QUESTION 191
Which of the following has the highest priority when defining an emergency response plan?

A. Critical data
B. Critical infrastructure
C. Safety of personnel
D. Vital records

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any

process or management practice. All of the other choices are secondary.

QUESTION 192
The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 193
The MOST important objective of a post incident review is to:

A. capture lessons learned to improve the process.
B. develop a process for continuous improvement.
C. develop a business case for the security program budget.
D. identify new incident management tools.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 194

Which of the following is the MOST critical consideration when collecting and preserving admissible evidence during an incident response?

A. Unplugging the systems
B. Chain of custody
C. Separation of duties
D. Clock synchronization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Admissible evidence must be collected and preserved by "chain of custody." Unplugging the systems can cause potential loss of information critical to the investigation. Separation of duties is not necessary in evidence collection and preservation since the entire process can be done by a single person. Clock synchronization is not as important for the collection and preservation of admissible evidence.

QUESTION 195
In a forensic investigation, which of the following would be the MOST important factor?

VCEplus
VCE To PDF - Free Practice Exam

A. Operation of a robust incident management process
B. Identification of areas of responsibility
C. Involvement of law enforcement
D. Expertise of resources

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The most important factor in a forensic investigation is the expertise of the resources participating in the project due to the inherent complexity. Operation of a robust incident management process and the identification of areas of responsibility should occur prior to an investigation. Involvement of law enforcement is dependent upon the nature of the investigation.

QUESTION 196
When a major vulnerability in the security of a critical web server is discovered, immediate notification should be made to the:

A. system owner to take corrective action.
B. incident response team to investigate.

C. data owners to mitigate damage.
D. development team to remediate.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to correct the vulnerabilities, the system owner needs to be notified quickly before an incident can take place. Choice B is not correct because the incident has not taken place and notification could delay implementation of the fix. Data owners would be notified only if the vulnerability could have compromised data. The development team may be called upon by the system owner to resolve the vulnerability.

QUESTION 197
Three employees reported the theft or loss of their laptops while on business trips. The FIRST course of action for the security manager is to:

A. assess the impact of the loss and determine mitigating steps.
B. communicate the best practices in protecting laptops to all laptop users.
C. instruct the erring employees to pay a penalty for the lost laptops.
D. recommend that management report the incident to the police and file for insurance.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The first step when addressing theft or loss is to figure out what was actually lost and what needs to occur in response. Choice B may occur after the impact is assessed. Choices C and D depend upon company policy.

QUESTION 198
Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 199
The FIRST step in an incident response plan is to:

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

Correct Answer: D
Section: (none)
Explanation

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

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 200
An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 201
Senior management commitment and support for information security can BEST be obtained through presentations that:

A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best security practices.
D. tie security risks to key business objectives.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
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:

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following will BEST protect an organization from internal security attacks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
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: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 205
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: (none)
Explanation

Explanation/Reference:

QUESTION 206
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

A. Business impact analysis (BIA)

B. Risk assessment
C. Vulnerability assessment
D. Business process mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
Acceptable risk is achieved when:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
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: (none)
Explanation

Explanation/Reference:

QUESTION 210
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:

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
Explanation

Explanation/Reference:

QUESTION 211
The MOST important component of a privacy policy is:

A. notifications.
B. warranties.
C. liabilities.
D. geographic coverage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
It is MOST important that information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 213
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: (none)
Explanation

Explanation/Reference:

QUESTION 214
An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Security technologies should be selected PRIMARILY on the basis of their:

A. ability to mitigate business risks.
B. evaluations in trade publications.
C. use of new and emerging technologies.
D. benefits in comparison to their costs.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
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: (none)
Explanation

Explanation/Reference:

QUESTION 217
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: (none)
Explanation

Explanation/Reference:

QUESTION 218
Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

VCEplus
VCE To PDF - Free Practice Exam

A. mandatory access controls.
B. discretionary access controls.
C. lattice-based access controls.
D. role-based access controls.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
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: (none)
Explanation

Explanation/Reference:

QUESTION 220
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: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 221
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: (none)
Explanation

Explanation/Reference:

QUESTION 222
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts
B. Write access violations
C. Concurrent logons
D. Firewall logs

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
The PRIMARY goal in developing an information security strategy is to:

A. establish security metrics and performance monitoring.
B. educate business process owners regarding their duties.
C. ensure that legal and regulatory requirements are met.
D. support the business objectives of the organization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
A risk assessment should be conducted:

A. once a year for each business process andsubprocess.
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.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
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: (none)
Explanation

Explanation/Reference:

QUESTION 228
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 229
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: (none)
Explanation

Explanation/Reference:

QUESTION 230
What is the BEST method for mitigating against network denial of service (DoS) attacks?

A. Ensure all servers are up-to-date on OS patches
B. Employ packet filtering to drop suspect packets
C. Implement network address translation to make internal addresses nonroutable
D. Implement load balancing for Internet facing devices

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
B. establish baseline standards for all locations and add supplemental standards as required.
C. bring all locations into conformity with a generally accepted set of industry best practices.
D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
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: (none)
Explanation

Explanation/Reference:

QUESTION 233
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: (none)
Explanation

Explanation/Reference:

QUESTION 234
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?

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
Explanation

Explanation/Reference:

QUESTION 235
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: (none)
Explanation

Explanation/Reference:

QUESTION 236
Which of the following is an inherent weakness of signature-based intrusion detection systems?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 237
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: (none)
Explanation

Explanation/Reference:

QUESTION 238
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: (none)
Explanation

Explanation/Reference:

QUESTION 239
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

VCEplus
VCE To PDF - Free Practice Exam

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks
C. Demonstrate that IT mitigating controls are in place
D. Suggest new IT controls to mitigate operational risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
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: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 242
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: (none)
Explanation

Explanation/Reference:

QUESTION 243
From an information security manager perspective, what is the immediate benefit of clearly- defined roles and responsibilities?

A. Enhanced policy compliance
B. Improved procedure flows
C. Segregation of duties
D. Better accountability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
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: (none)
Explanation

Explanation/Reference:

QUESTION 246
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: (none)
Explanation

Explanation/Reference:

QUESTION 247
Which of the following are the MOST important individuals to include as members of an information security steering committee?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)

D. Return on security investment report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
Which of the following is responsible for legal and regulatory liability?

A. Chief security officer (CSO)
B. Chief legal counsel (CLC)
C. Board and senior management
D. Information security steering group

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 250
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: (none)
Explanation

Explanation/Reference:

QUESTION 251

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
The FIRST priority when responding to a major security incident is:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
Who in an organization has the responsibility for classifying information?

A. Data custodian
B. Database administrator
C. Information security officer
D. Data owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
It is important to classify and determine relative sensitivity of assets to ensure that:

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
Explanation

Explanation/Reference:

QUESTION 256
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

VCEplus
VCE To PDF - Free Practice Exam

D. Measure the probability of occurrence of each threat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 258
Good information security standards should:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
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

VCEplus
VCE To PDF - Free Practice Exam

likely reason they made this decision is that:

A. thereare 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: (none)
Explanation

Explanation/Reference:

QUESTION 260
Logging is an example of which type of defense against systems compromise?

A. Containment
B. Detection
C. Reaction
D. Recovery

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
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: (none)
Explanation

Explanation/Reference:

QUESTION 262
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: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 263
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: (none)
Explanation

Explanation/Reference:

QUESTION 264
When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

A. Ensuring accessibility should a disasteroccur
B. Versioning control as plans are modified

C. Broken hyperlinks to resources stored elsewhere
D. Tracking changes in personnel and plan assets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
Which of the following is MOST important in developing a security strategy?

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

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 266
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: (none)
Explanation

Explanation/Reference:

QUESTION 267
Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the incident.
B. notify senior management.
C. start containment.
D. notify law enforcement.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
Which of the following factors is a primary driver for information security governance that does not require any further justification?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
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: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 271
What is the MOST appropriate change management procedure for the handling of emergency program changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

A. The right to conduct independent security reviews

B. A legally binding data protection agreement
C. Encryption between the organization and the provider
D. A joint risk assessment of the system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
A security manager meeting the requirements for the international flow of personal data will need to ensure:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
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: (none)
Explanation

Explanation/Reference:

QUESTION 275
When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
Which of the following provides the BEST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

VCEplus
VCE To PDF - Free Practice Exam

A. The recovery time objective (RTO) was not exceeded during testing
B. Objective testing of the business continuity/disaster recovery plan has been carried out consistently
C. The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
D. Information assets have been valued and assigned to owners per the business continuity plan/disaster recovery plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 279
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 280
Which of the following situations would be the MOST concern to a security manager?

A. Audit logs are not enabled on a production server
B. The logon ID for a terminated systems analyst still exists on the system
C. The help desk has received numerous results of users receiving phishing e-mails
D. A Trojan was found to be installed on a system administrator's laptop

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
Which of the following events generally has the highest information security impact?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 284
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
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: (none)
Explanation

Explanation/Reference:

QUESTION 286
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop

Correct Answer: D
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 287
What is the BEST way to alleviate security team understaffing while retaining the capability in- house?

A. Hire a contractor that would not be included in the permanent headcount
B. Outsource with a security services provider while retaining the control internally
C. Establish a virtual security team from competent employees across the company
D. Provide cross training to minimize the existing resources gap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
Which would be the BEST recommendation to protect against phishing attacks?

A. Install anantispam system
B. Publish security guidance for customers
C. Provide security awareness to the organization's staff
D. Install an application-level firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
To achieve effective strategic alignment of security initiatives, it is important that:

A. steering committee leadershipbe selected by rotation.
B. inputs be obtained and consensus achieved between the major organizational units.
C. the business strategybe updated periodically.
D. procedures and standardsbe approved by all departmental heads.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
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 are 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: (none)
Explanation

Explanation/Reference:

QUESTION 291
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

A. The program's governance oversight mechanisms
B. Information security periodicals and manuals
C. The program's security architecture and design
D. Training and certification of the information security team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 292
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: (none)
Explanation

Explanation/Reference:

QUESTION 293
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: (none)
Explanation

Explanation/Reference:

QUESTION 294
Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

A. Reconciliation of the annual systems inventory to the disaster recovery/business continuity plans
B. Periodic audits of the disaster recovery/business continuity plans
C. Comprehensive walk-through testing
D. Inclusion as a required step in the system life cycle process

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
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: (none)
Explanation

Explanation/Reference:

QUESTION 296
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
D. Require that a change request be submitted for each download

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 297
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

A. Budget allocation
B. Technical skills of staff
C. User acceptance
D. Password requirements

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
What is the GREATEST risk when there is an excessive number of firewall rules?

A. One rule may override another rule in the chain and create a loophole
B. Performance degradation of the whole network

C. The firewall may not support the increasing number of rules due to limitations
D. The firewall may show abnormal behavior and may crash or automatically shut down

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
What is the BEST way to ensure data protection upon termination of employment?

A. Retrieve identification badge and card keys
B. Retrieve all personal computer equipment
C. Erase all of the employee's folders
D. Ensure all logical access is removed

Correct Answer: D
Section: (none)
Explanation

VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 300
Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

A. Conduct awareness sessions on intellectual property policy
B. Require all employees to sign a nondisclosure agreement
C. Promptly remove all access when an employee leaves the organization
D. Restrict access to a need-to-know basis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)
D. Return on security investment report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Performing a risk assessment will allow the information security manager to prioritize the remedial measures and provide a means to convey a sense of urgency to management. Metrics reports are normally contained within the methodology of the risk assessment to give it credibility and provide an ongoing tool. The business impact analysis (BIA) covers continuity risks only. Return on security investment cannot be determined until a plan is developed based on the BIA.

QUESTION 302
Which of the following would be the FIRST step in establishing an information security program?

VCEplus
VCE To PDF - Free Practice Exam

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: (none)
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 303
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart

C. Gap analysis
D. Balanced scorecard

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
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: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference: