

## CISM Dumps

### Certified Information Security Manager

<https://www.certleader.com/CISM-dumps.html>



**NEW QUESTION 1**

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- A. Regular password audits
- B. Single sign-on system
- C. Security awareness program
- D. Penalties for noncompliance

**Answer: C**

**Explanation:**

To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

**NEW QUESTION 2**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 3**

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

**Answer: D**

**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.

**NEW QUESTION 4**

Which of the following would BEST ensure the success of information security governance within an organization?

- A. Steering committees approve security projects
- B. Security policy training provided to all managers
- C. Security training available to all employees on the intranet
- D. Steering committees enforce compliance with laws and regulations

**Answer: A**

**Explanation:**

The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. Compliance with laws and regulations is part of the responsibility of the steering committee but it is not a full answer. Awareness training is important at all levels in any medium, and also an indicator of good governance. However, it must be guided and approved as a security project by the steering committee.

**NEW QUESTION 5**

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

**Answer: C**

**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.

**NEW QUESTION 6**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 7**

Investments in information security technologies should be based on:

- A. vulnerability assessment
- B. value analysis
- C. business climate
- D. audit recommendation

**Answer: B**

**Explanation:**

Investments in security technologies should be based on a value analysis and a sound business case. Demonstrated value takes precedence over the current business climate because it is ever changing. Basing decisions on audit recommendations would be reactive in nature and might not address the key business needs comprehensively. Vulnerability assessments are useful, but they do not determine whether the cost is justified.

**NEW QUESTION 8**

Which of the following MOST commonly falls within the scope of an information security governance steering committee?

- A. Interviewing candidates for information security specialist positions
- B. Developing content for security awareness programs
- C. Prioritizing information security initiatives
- D. Approving access to critical financial systems

**Answer: C**

**Explanation:**

Prioritizing information security initiatives is the only appropriate item. The interviewing of specialists should be performed by the information security manager, while the developing of program content should be performed by the information security staff. Approving access to critical financial systems is the responsibility of individual system data owners.

**NEW QUESTION 9**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 10**

The PRIMARY objective of a security steering group is to:

- A. ensure information security covers all business functions
- B. ensure information security aligns with business goals
- C. raise information security awareness across the organization
- D. implement all decisions on security management across the organization

**Answer:** B

**Explanation:**

The security steering group comprises senior management of key business functions and has the primary objective to align the security strategy with the business direction. Option A is incorrect because all business areas may not be required to be covered by information security; but, if they do, the main purpose of the steering committee would be alignment more so than coverage. While raising awareness is important, this goal would not be carried out by the committee itself. The steering committee may delegate part of the decision making to the information security manager; however, if it retains this authority, it is not the primary' goal.

#### **NEW QUESTION 10**

Information security governance is PRIMARILY driven by:

- A. technology constraint
- B. regulatory requirement
- C. litigation potentia
- D. business strateg

**Answer:** D

**Explanation:**

Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily in line with the business strategy.

#### **NEW QUESTION 13**

Which of the following is the MOST important factor when designing information security architecture?

- A. Technical platform interfaces
- B. Scalability of the network
- C. Development methodologies
- D. Stakeholder requirements

**Answer:** D

**Explanation:**

The most important factor for information security is that it advances the interests of the business, as defined by stakeholder requirements. Interoperability and scalability, as well as development methodologies, are all important but are without merit if a technologically-elegant solution is achieved that does not meet the needs of the business.

#### **NEW QUESTION 14**

Which of the following are likely to be updated MOST frequently?

- A. Procedures for hardening database servers
- B. Standards for password length and complexity
- C. Policies addressing information security governance
- D. Standards for document retention and destruction

**Answer:** A

**Explanation:**

Policies and standards should generally be more static and less subject to frequent change. Procedures on the other hand, especially with regard to the hardening of operating systems, will be subject to constant change; as operating systems change and evolve, the procedures for hardening will have to keep pace.

#### **NEW QUESTION 16**

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

- A. establish security metrics and performance monitorin
- B. educate business process owners regarding their dutie
- C. ensure that legal and regulatory requirements are met
- D. support the business objectives of the organizatio

**Answer:** D

**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.

#### **NEW QUESTION 17**

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

**Answer:** C

**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.

#### **NEW QUESTION 18**

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

**Answer:** A

**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.

#### **NEW QUESTION 21**

Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

- A. Update platform-level security settings
- B. Conduct disaster recovery test exercises
- C. Approve access to critical financial systems
- D. Develop an information security strategy paper

**Answer:** D

**Explanation:**

Developing a strategy paper on information security would be the most appropriate. Approving access would be the job of the data owner. Updating platform-level security and conducting recovery test exercises would be less essential since these are administrative tasks.

#### **NEW QUESTION 22**

A good privacy statement should include:

- A. notification of liability on accuracy of informatio
- B. notification that information will be encrypte
- C. what the company will do with information it collect
- D. a description of the information classification proces

**Answer:** C

**Explanation:**

Most privacy laws and regulations require disclosure on how information will be used. Choice A is incorrect because that information should be located in the web site's disclaimer. Choice B is incorrect because, although encryption may be applied, this is not generally disclosed. Choice D is incorrect because information classification would be contained in a separate policy.

#### **NEW QUESTION 24**

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

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

**Answer:** C

**Explanation:**

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

#### **NEW QUESTION 29**

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 standard
- 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 requirement

**Answer:** D

**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.

#### **NEW QUESTION 33**

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

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

**Answer:** A

**Explanation:**

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

#### **NEW QUESTION 36**

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

**Answer:** D

**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.

#### **NEW QUESTION 37**

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

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

**Answer:** D

**Explanation:**

The steering committee controls the execution of the information security strategy, according to the needs of the organization, and decides on the project prioritization and the execution plan. User management is an important group that should be represented to ensure that the information security plans are aligned with the business needs. Functional requirements and user training programs are considered to be part of the projects but are not the main risks. The steering committee does not approve budgets for business units.

#### **NEW QUESTION 38**

Which of the following should be the FIRST step in developing an information security plan?

- A. Perform a technical vulnerabilities assessment
- B. Analyze the current business strategy
- C. Perform a business impact analysis
- D. Assess the current levels of security awareness

**Answer:** B

**Explanation:**

Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business



strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

**NEW QUESTION 41**

When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

- A. Develop a security architecture
- B. Establish good communication with steering committee members
- C. Assemble an experienced staff
- D. Benchmark peer organizations

**Answer: B**

**Explanation:**

New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support. Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

**NEW QUESTION 46**

Which of the following requirements would have the lowest level of priority in information security?

- A. Technical
- B. Regulatory
- C. Privacy
- D. Business

**Answer: A**

**Explanation:**

Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

**NEW QUESTION 51**

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

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

**Answer: C**

**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.

**NEW QUESTION 52**

Which of the following would be the MOST important goal of an information security governance program?

- A. Review of internal control mechanisms
- B. Effective involvement in business decision making
- C. Total elimination of risk factors
- D. Ensuring trust in data

**Answer: D**

**Explanation:**

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true. Involvement in decision making is important only to ensure business data integrity so that data can be trusted.

**NEW QUESTION 54**

Senior management commitment and support for information security can BEST be enhanced through:

- A. a formal security policy sponsored by the chief executive officer (CEO).
- B. regular security awareness training for employee
- C. periodic review of alignment with business management goal
- D. senior management signoff on the information security strateg

**Answer: C**

**Explanation:**

Ensuring that security activities continue to be aligned and support business goals is critical to obtaining their support. Although having the chief executive officer (CEO) signoff on the security policy and senior management signoff on the security strategy makes for good visibility and demonstrates good tone at the top, it is a one-time discrete event that may be quickly forgotten by senior management. Security awareness training for employees will not have as much effect on senior management commitment.

**NEW QUESTION 58**

Information security projects should be prioritized on the basis of:

- A. time required for implementatio
- B. impact on the organizatio
- C. total cost for implementatio
- D. mix of resources require

**Answer:** B  
**Explanation:**

**Explanation:**

Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

**NEW QUESTION 60**

Acceptable risk is achieved when:

- A. residual risk is minimize
- B. transferred risk is minimize
- C. control risk is minimize
- D. inherent risk is minimize

**Answer:** A

**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.

**NEW QUESTION 65**

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

- A. map the major threats to business objective
- B. review available sources of risk informatio
- C. identify the value of the critical asset
- D. determine the financial impact if threats materializ

**Answer:** A

**Explanation:**

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

**NEW QUESTION 68**

Risk management programs are designed to reduce risk to:

- A. a level that is too small to be measurabl
- B. the point at which the benefit exceeds the expens
- C. a level that the organization is willing to accep
- D. a rate of return that equals the current cost of capita

**Answer:** C

**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.

**NEW QUESTION 72**

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- A. Recover)' time objective (RTO)
- B. Maximum tolerable outage (MTO)
- C. Recovery point objectives (RPOs)
- D. Services delivery objectives (SDOs)



**Answer:** A

**Explanation:**

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

**NEW QUESTION 76**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 80**

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 83**

Risk acceptance is a component of which of the following?

- A. Assessment
- B. Mitigation
- C. Evaluation
- D. Monitoring

**Answer:** B

**Explanation:**

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

**NEW QUESTION 88**

Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

- A. Defining job roles
- B. Performing a risk assessment
- C. Identifying data owners
- D. Establishing data retention policies

**Answer:** C

**Explanation:**

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

**NEW QUESTION 91**

A successful risk management program should lead to:

- A. optimization of risk reduction efforts against costs
- 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 risk

**Answer:** A

**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.

#### NEW QUESTION 94

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

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

**Answer:** A

**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.

#### NEW QUESTION 95

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 97

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 100

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 104

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

**Answer:** B

**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.

#### NEW QUESTION 108

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

- A. cost of protection is in proportion to sensitivit
- B. highly sensitive assets are protecte
- C. cost of controls is minimize
- D. countermeasures are proportional to ris

**Answer:** D

**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.

#### NEW QUESTION 113

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 115

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

**Answer:** A

**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.

#### NEW QUESTION 118

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

- A. Implement countermeasure
- B. Eliminate the ris
- C. Transfer the ris
- D. Accept the ris

**Answer:** C

**Explanation:**

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

**NEW QUESTION 119**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 120**

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

**Answer: B**

**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.

**NEW QUESTION 123**

The valuation of IT assets should be performed by:

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 127**

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

**Answer: A**

**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.

**NEW QUESTION 132**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 135**

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

- A. organizational requirement
- B. information systems requirement
- C. information security requirement
- D. international standard

**Answer:** A

**Explanation:**

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

**NEW QUESTION 137**

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

- A. Staff interviews
- B. Threat identification
- C. Asset identification and valuation
- D. Determination of the likelihood of identified risks

**Answer:** C

**Explanation:**

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

**NEW QUESTION 139**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 144**

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

- A. total cost of ownershi
- B. priority of restoratio
- C. annualized loss expectancy (ALE).
- D. residual ris

**Answer:** B

**Explanation:**

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

**NEW QUESTION 145**

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

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

**Answer:** D



**Explanation:**

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

**NEW QUESTION 146**

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

- A. minimizing operational impact
- B. eliminating all vulnerabilities
- C. usage by similar organization
- D. certification from a third party

**Answer:** A

**Explanation:**

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

**NEW QUESTION 150**

Who is responsible for ensuring that information is classified?

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

**Answer:** C

**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.

**NEW QUESTION 151**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 152**

An information security organization should PRIMARILY:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 156**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 160**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 161**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 162**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 165**

In assessing risk, it is MOST essential to:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 167**

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

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

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 169**

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

**Answer:** C

**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.

#### **NEW QUESTION 174**

Identification and prioritization of business risk enables project managers to:

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

**Answer:** C

**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.

#### **NEW QUESTION 177**

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

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

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 181**

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

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

**Answer:** C

**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.

#### **NEW QUESTION 182**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 183**

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

- A. password reset
- B. reported incident
- C. incidents resolved
- D. access rule violation

**Answer: B**

**Explanation:**

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

**NEW QUESTION 188**

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

**Answer: A**

**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.

**NEW QUESTION 189**

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

- A. Patch management
- B. Change management
- C. Security metrics
- D. Version control

**Answer: B**

**Explanation:**

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

**NEW QUESTION 190**

An information security program should be sponsored by:

- A. infrastructure management
- B. the corporate audit department
- C. key business process owner
- D. information security management

**Answer: C**

**Explanation:**

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

**NEW QUESTION 194**

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 197

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

**Answer:** D

**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.

#### NEW 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:

- A. broken authenticatio
- B. unvalidated inpu
- C. cross-site scriptin
- D. structured query language (SQL) injectio

**Answer:** A

**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.

#### NEW QUESTION 203

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

- A. develop a risk assessment pla
- B. develop a data protection pla
- C. protect information assets and resource
- D. establish security governanc

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 207

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

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

**Answer:** D

**Explanation:**

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



**NEW QUESTION 208**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 209**

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

**Answer: D**

**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.

**NEW QUESTION 210**

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

- A. authentication and authorizatio
- B. confidentiality and integrit
- C. confidentiality and nonrepudiatio
- D. authentication and nonrepudiatio

**Answer: C**

**Explanation:**

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

**NEW QUESTION 212**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 214**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 219**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 224**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 229**

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

- A. change the root password of the syste
- B. implement multifactor authenticatio
- C. rebuild the system from the original installation mediu
- D. disconnect the mail server from the networ

**Answer:** C

**Explanation:**

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

**NEW QUESTION 231**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 233**

Nonrepudiation can BEST be ensured by using:

- A. strong password
- B. a digital has
- C. symmetric encryptio
- D. digital signature

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 234**

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

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

**Answer:** C

**Explanation:**

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

#### **NEW QUESTION 235**

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 processes

**Answer:** A

**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.

#### **NEW QUESTION 236**

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

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

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 240**

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

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

**Answer:** A

**Explanation:**

Login 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.

#### **NEW QUESTION 245**

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

- A. access to inappropriate site
- B. downloading malicious cod
- C. violation of copyright law
- D. disruption of Internet acces

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 247**

An intranet server should generally be placed on the:

- A. internal networ
- B. firewall serve
- C. external route
- D. primary domain controlle

**Answer:** A

**Explanation:**

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

#### **NEW QUESTION 250**

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

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 255**

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

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 256**

Which of the following is the BEST indicator that an effective security control is built into an organization?

- A. The monthly service level statistics indicate a minimal impact from security issue
- B. The cost of implementing a security control is less than the value of the asset
- C. The percentage of systems that is compliant with security standard
- D. The audit reports do not reflect any significant findings on securit

**Answer:** A

**Explanation:**

The best indicator of effective security control is the evidence of little disruption to business operations. Choices B, C and D can support this evidence, but are supplemental to choice A.

#### **NEW QUESTION 259**

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

- A. report risks in other department
- B. obtain support from other department
- C. report significant security risk
- D. have knowledge of security standard

**Answer:** C

**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.

#### **NEW QUESTION 264**

The MOST important reason for formally documenting security procedures is to ensure:

- A. processes are repeatable and sustainable
- B. alignment with business objective
- C. auditability by regulatory agencies
- D. objective criteria for the application of metrics

**Answer:** A

**Explanation:**

Without formal documentation, it would be difficult to ensure that security processes are performed in the proper manner every time that they are performed. Alignment with business objectives is not a function of formally documenting security procedures. Processes should not be formally documented merely to satisfy an audit requirement. Although potentially useful in the development of metrics, creating formal documentation to assist in the creation of metrics is a secondary objective.

#### **NEW QUESTION 266**

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

**Answer:** B

**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.

#### **NEW QUESTION 267**

Security awareness training should be provided to new employees:

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

**Answer:** C

**Explanation:**

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

#### **NEW QUESTION 271**

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

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

**Answer:** C

**Explanation:**

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



**NEW QUESTION 276**

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

- A. similar change request
- B. change request postponement
- C. canceled change request
- D. emergency change request

**Answer:** D

**Explanation:**

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

**NEW QUESTION 280**

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

**Answer:** A

**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.

**NEW QUESTION 283**

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

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

**Answer:** D

**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.

**NEW QUESTION 284**

Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

- A. policy
- B. strategy
- C. guideline
- D. baseline

**Answer:** A

**Explanation:**

A security policy is a general statement to define management objectives with respect to security. The security strategy addresses higher level issues. Guidelines are optional actions and operational tasks. A security baseline is a set of minimum requirements that is acceptable to an organization.

**NEW QUESTION 287**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 288**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 293**

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 syste
- B. sustaining the organization's security postur
- C. the existing systems that will be affecte
- D. complying with segregation of dutie

**Answer:** B

**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).

**NEW QUESTION 296**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 300**

Information security policies should:

- A. address corporate network vulnerabilitie
- B. address the process for communicating a violatio
- C. be straightforward and easy to understan
- D. be customized to specific groups and role

**Answer:** C

**Explanation:**

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

**NEW QUESTION 305**

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

- A. Standards
- B. Guidelines
- C. Security metrics
- D. IT governance

**Answer:** A

**Explanation:**

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

**NEW QUESTION 310**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 315**

Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

- A. Security audit reports
- B. Balanced scorecard
- C. Capability maturity model (CMM)
- D. Systems and business security architecture

**Answer: C**

**Explanation:**

The capability maturity model (CMM) grades each defined area of security processes on a scale of 0 to 5 based on their maturity, and is commonly used by entities to measure their existing state and then determine the desired one. Security audit reports offer a limited view of the current state of security. Balanced scorecard is a document that enables management to measure the implementation of their strategy and assists in its translation into action. Systems and business security architecture explain the security architecture of an entity in terms of business strategy, objectives, relationships, risks, constraints and enablers, and provides a business-driven and business-focused view of security architecture.

**NEW QUESTION 319**

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

**Answer: A**

**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.

**NEW QUESTION 320**

Security policies should be aligned MOST closely with:

- A. industry' best practice
- B. organizational need
- C. generally accepted standard
- D. local laws and regulation

**Answer: B**

**Explanation:**

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

**NEW QUESTION 324**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 328**

An information security program should focus on:

- A. best practices also in place at peer companie
- B. solutions codified in international standard
- C. key controls identified in risk assessment
- D. continued process improvemen

**Answer: C**

**Explanation:**

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

**NEW QUESTION 331**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 332**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 334**

In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

- A. testing time window prior to deploymen
- B. technical skills of the team responsibl
- C. certification of validity for deploymen
- D. automated deployment to all the server

**Answer: A**

**Explanation:**

Having the patch tested prior to implementation on critical systems is an absolute prerequisite where availability is a primary concern because deploying patches that could cause a system to fail could be worse than the vulnerability corrected by the patch. It makes no sense to deploy patches on every system. Vulnerable systems should be the only candidate for patching. Patching skills are not required since patches are more often applied via automated tools.

**NEW QUESTION 335**

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

- A. business process owner
- B. the information security manage
- C. the security steering committe
- D. IT senior managemen

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 337**

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

**Answer:** D

**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.

#### **NEW QUESTION 339**

Successful social engineering attacks can BEST be prevented through:

- A. preemployment screenin
- B. close monitoring of users' access pattern
- C. periodic awareness trainin
- D. efficient termination procedure

**Answer:** C

**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.

#### **NEW QUESTION 341**

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

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

**Answer:** C

**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.

#### **NEW QUESTION 346**

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

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

**Answer:** D

**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.

#### **NEW QUESTION 348**

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

- A. User passwords are not automatically expired



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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 353

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 risk
- C. isolate the system from the rest of the network
- D. request a risk acceptance from senior management

**Answer:** B

**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.

#### NEW QUESTION 356

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

- A. Key metrics indicate a reduction in incident impact
- B. Senior management has approved the program and is supportive of it
- C. Employees are receptive to changes that were implemented
- D. There is an immediate reduction in reported incidents

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 359

Data owners are normally responsible for which of the following?

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 363

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 366

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

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 368**

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

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

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 372**

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

**Answer:** B

**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.

#### **NEW QUESTION 373**

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

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

**Answer:** C

**Explanation:**

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

#### **NEW QUESTION 376**

Which of the following is MOST important to the successful promotion of good security management practices?

- A. Security metrics
- B. Security baselines
- C. Management support
- D. Periodic training

**Answer:** C

**Explanation:**

Without management support, all other efforts will be undermined. Metrics, baselines and training are all important, but they depend on management support for their success.

#### **NEW QUESTION 378**

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

the BEST solution?

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

**Answer: B**

**Explanation:**

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

#### **NEW QUESTION 381**

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

- A. source routing
- B. broadcast propagation
- C. unregistered port
- D. nonstandard protocol

**Answer: A**

**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.

#### **NEW QUESTION 384**

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

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

**Answer: A**

**Explanation:**

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

#### **NEW QUESTION 388**

The PRIMARY objective of security awareness is to:

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

**Answer: B**

**Explanation:**

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

#### **NEW QUESTION 393**

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

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

**Answer: C**

**Explanation:**

Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security

requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

**NEW QUESTION 396**

When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

- A. Business continuity plan
- B. Disaster recovery plan
- C. Incident response plan
- D. Vulnerability management plan

**Answer:** C

**Explanation:**

An incident response plan documents the step-by-step process to follow, as well as the related roles and responsibilities pertaining to all parties involved in responding to an information security breach. A business continuity plan or disaster recovery plan would be triggered during the execution of the incident response plan in the case of a breach impacting the business continuity. A vulnerability management plan is a procedure to address technical vulnerabilities and mitigate the risk through configuration changes (patch management).

**NEW QUESTION 399**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 402**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 407**

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 incident
- B. obtain support for enhancing the expertise of the third-party team
- C. identify lessons learned for further improving the information security management process
- D. obtain better buy-in for the information security program

**Answer:** A

**Explanation:**

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

**NEW QUESTION 408**

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

**Answer:** C

**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.

#### **NEW QUESTION 411**

The PRIORITY action to be taken when a server is infected with a virus is to:

- A. isolate the infected server(s) from the network
- B. identify all potential damage caused by the infection
- C. ensure that the virus database files are current
- D. establish security weaknesses in the firewall

**Answer:** A

**Explanation:**

The priority in this event is to minimize the effect of the virus infection and to prevent it from spreading by removing the infected server(s) from the network. After the network is secured from further infection, the damage assessment can be performed, the virus database updated and any weaknesses sought.

#### **NEW QUESTION 413**

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

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 416**

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

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

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 417**

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)

**Answer:** C

**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.

#### **NEW QUESTION 419**

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

- A. Quarantine all picture files stored on file servers
- B. Block all e-mails containing picture file attachments



- C. Quarantine all mail servers connected to the Internet
- D. Block incoming Internet mail, but permit outgoing mail

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 420**

Why is "slack space" of value to an information security manager as part of an incident investigation?

- A. Hidden data may be stored there
- B. The slack space contains login information
- C. Slack space is encrypted
- D. It provides flexible space for the investigation

**Answer:** A

**Explanation:**

"Slack space" is the unused space between where the file data ends and the end of the cluster the data occupies. Login information is not typically stored in the slack space. Encryption for the slack space is no different from the rest of the file system. The slack space is not a viable means of storage during an investigation.

#### **NEW QUESTION 425**

Which of the following application systems should have the shortest recovery time objective (RTO)?

- A. Contractor payroll
- B. Change management
- C. E-commerce web site
- D. Fixed asset system

**Answer:** C

**Explanation:**

In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours, if not minutes. Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

#### **NEW QUESTION 426**

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

**Answer:** C

**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.

#### **NEW QUESTION 427**

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

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

**Answer:** C

**Explanation:**

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

#### **NEW QUESTION 431**

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 tape

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

**Answer:** B

**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.

#### **NEW QUESTION 435**

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 caus
- B. discontinue the use of the vulnerable technolog
- C. report to senior management that the organization is not affecte
- D. remind staff that no similar security breaches have taken plac

**Answer:** A

**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.

#### **NEW QUESTION 440**

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

- A. Copies of critical contracts and service level agreements (SLAs)
- B. Copies of the business continuity plan
- C. Key software escrow agreements for the purchased systems
- D. List of emergency numbers of service providers

**Answer:** B

**Explanation:**

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

#### **NEW QUESTION 445**

Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

- A. A bit-level copy of all hard drive data
- B. The last verified backup stored offsite
- C. Data from volatile memory
- D. Backup servers

**Answer:** A

**Explanation:**

The bit-level copy image file ensures forensic quality evidence that is admissible in a court of law. Choices B and D may not provide forensic quality data for investigative work, while choice C alone may not provide enough evidence.

#### **NEW QUESTION 448**

An intrusion detection system (IDS) should:

- A. run continuously
- B. ignore anomalies
- C. require a stable, rarely changed environment
- D. be located on the network

**Answer:** A

**Explanation:**

If an intrusion detection system (IDS) does not run continuously the business remains vulnerable. An IDS should detect, not ignore anomalies. An IDS should be flexible enough to cope with a changing environment. Both host and network based IDS are recommended for adequate detection.

#### **NEW QUESTION 452**

Which of the following would be MOST appropriate for collecting and preserving evidence?

- A. Encrypted hard drives
- B. Generic audit software
- C. Proven forensic processes
- D. Log correlation software

**Answer:** C

**Explanation:**

When collecting evidence about a security incident, it is very important to follow appropriate forensic procedures to handle electronic evidence by a method approved by local jurisdictions. All other options will help when collecting or preserving data about the incident; however these data might not be accepted as evidence in a court of law if they are not collected by a method approved by local jurisdictions.

**NEW QUESTION 457**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CISM Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CISM-dumps.html>