



**Isaca**

## **Exam Questions CISM**

Certified Information Security Manager

#### NEW QUESTION 1

When an organization is implementing an information security governance program, its board of directors should be responsible for:

- A. drafting information security policie
- B. reviewing training and awareness program
- C. setting the strategic direction of the progra
- D. auditing for complianc

**Answer: C**

#### Explanation:

A board of directors should establish the strategic direction of the program to ensure that it is in sync with the company's vision and business goals. The board must incorporate the governance program into the overall corporate business strategy. Drafting information security policies is best fulfilled by someone such as a security manager with the expertise to bring balance, scope and focus to the policies. Reviewing training and awareness programs may best be handled by security management and training staff to ensure that the training is on point and follows best practices. Auditing for compliance is best left to the internal and external auditors to provide an objective review of the program and how it meets regulatory and statutory compliance.

#### NEW QUESTION 2

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 3

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 4

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 5

The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

- A. the plan aligns with the organization's business pla
- B. departmental budgets are allocated appropriately to pay for the pla
- C. regulatory oversight requirements are me
- D. the impact of the plan on the business units is reduce

**Answer: A**

#### 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. The steering committee does not allocate department budgets for business units. While ensuring that regulatory oversight requirements are met could be a consideration, it is not the main reason for the review. Reducing the impact on the business units is a secondary concern but not the main reason for the review.

#### NEW QUESTION 6

Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

- A. Obtain the support of the board of director
- B. Improve the content of the information security awareness progra
- C. Improve the employees' knowledge of security policie
- D. Implement logical access controls to the information system

**Answer:** A

#### Explanation:

It is extremely difficult to implement an information security program without the aid and support of the board of directors. If they do not understand the importance of security to the achievement of the business objectives, other measures will not be sufficient. Options B and C are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

#### NEW QUESTION 7

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 8

A business unit intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should an information security manager take?

- A. Enforce the existing security standard
- B. Change the standard to permit the deployment
- C. Perform a risk analysis to quantify the risk
- D. Perform research to propose use of a better technology

**Answer:** C

#### Explanation:

Resolving conflicts of this type should be based on a sound risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. A blanket decision should never be given without conducting such an analysis. Enforcing existing standards is a good practice; however, standards need to be continuously examined in light of new technologies and the risks they present. Standards should not be changed without an appropriate risk assessment.

#### NEW QUESTION 9

The PRIMARY objective of a security steering group is to:

- A. ensure information security covers all business function
- B. ensure information security aligns with business goal
- C. raise information security awareness across the organizatio
- D. implement all decisions on security management across the organizatio

**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

A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

- A. meet with stakeholders to decide how to compl
- B. analyze key risks in the compliance proces
- C. assess whether existing controls meet the regulatio
- D. update the existing security/privacy polic

**Answer: C**

#### Explanation:

If the organization is in compliance through existing controls, the need to perform other work related to the regulation is not a priority. The other choices are appropriate and important; however, they are actions that are subsequent and will depend on whether there is an existing control gap.

#### NEW QUESTION 10

When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

- A. aligned with the IT strategic pla
- B. based on the current rate of technological chang
- C. three-to-five years for both hardware and softwar
- D. aligned with the business strateg

**Answer: D**

#### Explanation:

Any planning for information security should be properly aligned with the needs of the business. Technology should not come before the needs of the business, nor should planning be done on an artificial timetable that ignores business needs.

#### NEW QUESTION 15

Information security policy enforcement is the responsibility of the:

- A. security steering committe
- B. chief information officer (CIO).
- C. chief information security officer (CISO).
- D. chief compliance officer (CCO).

**Answer: C**

#### Explanation:

Information security policy enforcement is the responsibility of the chief information security officer (CISO), first and foremost. The board of directors and executive management should ensure that a security policy is in line with corporate objectives. The chief information officer (CIO) and the chief compliance officer (CCO) are involved in the enforcement of the policy but are not directly responsible for it.

#### NEW QUESTION 16

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 17

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

- A. It is easier to promote security awarenes
- B. It is easier to manage and contro
- C. It is more responsive to business unit need
- D. It provides a faster turnaround for security request

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 19

Which of the following is the MOST important information to include in an information security standard?

- A. Creation date
- B. Author name
- C. Initial draft approval date
- D. Last review date

**Answer:** D

#### Explanation:

The last review date confirms the currency of the standard, affirming that management has reviewed the standard to assure that nothing in the environment has changed that would necessitate an update to the standard. The name of the author as well as the creation and draft dates are not that important.

#### NEW QUESTION 23

Which of the following is the MOST important information to include in a strategic plan for information security?

- A. Information security staffing requirements
- B. Current state and desired future state
- C. IT capital investment requirements
- D. information security mission statement

**Answer:** B

#### Explanation:

It is most important to paint a vision for the future and then draw a road map from the stalling point to the desired future state. Staffing, capital investment and the mission all stem from this foundation.

#### NEW QUESTION 28

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 30

Effective IT governance is BEST ensured by:

- A. utilizing a bottom-up approach
- B. management by the IT department
- C. referring the matter to the organization's legal department
- D. utilizing a top-down approach

**Answer:** D

#### Explanation:

Effective IT governance needs to be a top-down initiative, with the board and executive management setting clear policies, goals and objectives and providing for ongoing monitoring of the same. Focus on the regulatory issues and management priorities may not be reflected effectively by a bottom-up approach. IT governance affects the entire organization and is not a matter concerning only the management of IT. The legal department is part of the overall governance process, but cannot take full responsibility.

#### NEW QUESTION 33

The MOST basic requirement for an information security governance program is to:

- A. be aligned with the corporate business strategy
- B. be based on a sound risk management approach
- C. provide adequate regulatory compliance
- D. provide best practices for security- initiative

**Answer:** A

#### Explanation:

To receive senior management support, an information security program should be aligned with the corporate business strategy. Risk management is a requirement of an information security program which should take into consideration the business strategy. Security governance is much broader than just regulatory compliance. Best practice is an operational concern and does not have a direct impact on a governance program.

#### NEW QUESTION 38

While implementing information security governance an organization should FIRST:

- A. adopt security standard
- B. determine security baseline
- C. define the security strateg
- D. establish security policie

**Answer: C**

#### Explanation:

The first step in implementing information security governance is to define the security strategy based on which security baselines are determined. Adopting suitable security-standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

#### NEW QUESTION 39

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

- A. establishing a periodic risk assessmen
- B. promoting regulatory requirement
- C. developing a business cas
- D. developing effective metric

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 43

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

- A. Examples of genuine incidents at similar organizations
- B. Statement of generally accepted best practices
- C. Associating realistic threats to corporate objectives
- D. Analysis of current technological exposures

**Answer: C**

#### Explanation:

Linking realistic threats to key business objectives will direct executive attention to them. All other options are supportive but not of as great a value as choice C when trying to obtain the funds for a new program.

#### NEW QUESTION 48

Who is ultimately responsible for the organization's information?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 52

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

- A. develop a security architectur
- B. install a network intrusion detection system (NIDS) and prepare a list of attack
- C. develop a network security polic
- D. conduct a risk assessmen

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 57

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

- A. performance measuremen
- B. integratio
- C. alignmen
- D. value deliver

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 59

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 62

Retention of business records should PRIMARILY be based on:

- A. business strategy and directio
- B. regulatory and legal requirement
- C. storage capacity and longevit
- D. business ease and value analysi

**Answer: B**

#### Explanation:

Retention of business records is generally driven by legal and regulatory requirements. Business strategy and direction would not normally apply nor would they override legal and regulatory requirements. Storage capacity and longevity are important but secondary issues. Business case and value analysis would be secondary to complying with legal and regulatory requirements.

#### NEW QUESTION 65

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

- A. Steering committee leadership be selected by rotatio
- B. Inputs be obtained and consensus achieved between the major organizational unit
- C. The business strategy be updated periodical
- D. Procedures and standards be approved by all departmental head

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 67

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 syste
- C. Existence of an alternate hot site in case of business disruptio
- 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 70**

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 74**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 76**

The MOST important component of a privacy policy is:

- A. notification
- B. warranty
- C. liability
- D. geographic coverage

**Answer:** A

**Explanation:**

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

**NEW QUESTION 79**

Which of the following is MOST appropriate for inclusion in an information security strategy?

- A. Business controls designated as key controls
- B. Security processes, methods, tools and techniques
- C. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
- D. Budget estimates to acquire specific security tools

**Answer:** B

**Explanation:**

A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to periodic change, and are not appropriate content for a strategy document.

#### NEW QUESTION 81

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 83

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

- A. attributes and characteristics of the 'desired state.'
- B. overall control objectives of the security progra
- C. mapping the IT systems to key business processe
- D. calculation of annual loss expectation

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 86

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 87

Which of the following roles would represent a conflict of interest for an information security manager?

- A. Evaluation of third parties requesting connectivity
- B. Assessment of the adequacy of disaster recovery plans
- C. Final approval of information security policies
- D. Monitoring adherence to physical security controls

**Answer:** C

#### Explanation:

Since management is ultimately responsible for information security, it should approve information security policy statements; the information security manager should not have final approval. Evaluation of third parties requesting access, assessment of disaster recovery plans and monitoring of compliance with physical security controls are acceptable practices and do not present any conflicts of interest.

#### NEW QUESTION 89

Who in an organization has the responsibility for classifying information?

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

**Answer:** D

#### Explanation:

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

### NEW QUESTION 93

Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

- A. More uniformity in quality of service
- B. Better adherence to policies
- C. Better alignment to business unit needs
- D. More savings in total operating costs

**Answer: C**

#### Explanation:

Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

### NEW QUESTION 95

When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

- A. Business management
- B. Operations manager
- C. Information security manager
- D. System users

**Answer: C**

#### Explanation:

The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

### NEW QUESTION 96

Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

- A. Information security manager
- B. Chief operating officer (COO)
- C. Internal auditor
- D. Legal counsel

**Answer: B**

#### Explanation:

The chief operating officer (COO) is highly-placed within an organization and has the most knowledge of business operations and objectives. The chief internal auditor and chief legal counsel are appropriate members of such a steering group. However, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since a security manager is looking to this group for direction, they are not in the best position to oversee formation of this group.

### NEW QUESTION 97

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

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

**Answer: C**

#### Explanation:

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

### NEW QUESTION 102

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 106

Which of the following authentication methods prevents authentication replay?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 108

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 109

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 110

The PRIMARY purpose of using risk analysis within a security program is to:

- A. justify the security expenditur
- B. help businesses prioritize the assets to be protecte
- C. inform executive management of residual risk valu
- D. assess exposures and plan remediatio

**Answer: D**

#### Explanation:

Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

#### NEW QUESTION 112

One way to determine control effectiveness is by determining:

- A. whether it is preventive, detective or compensator
- B. the capability of providing notification of failur
- C. the test results of intended objective
- D. the evaluation and analysis of reliabilit

**Answer:**

C

**Explanation:**

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

**NEW QUESTION 115**

The BEST strategy for risk management is to:

- A. achieve a balance between risk and organizational goal
- B. reduce risk to an acceptable level
- C. ensure that policy development properly considers organizational risk
- D. ensure that all unmitigated risks are accepted by management

**Answer: B**

**Explanation:**

The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to be considered a strategy.

**NEW QUESTION 120**

The MOST effective use of a risk register is to:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 123**

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

- A. Disclosure of personal information
- B. Sufficient coverage of the insurance policy for accidental losses
- C. Intrinsic value of the data stored on the equipment
- D. Replacement cost of the equipment

**Answer: C**

**Explanation:**

When mobile equipment is lost or stolen, the information contained on the equipment matters most in determining the impact of the loss. The more sensitive the information, the greater the liability. If staff carries mobile equipment for business purposes, an organization must develop a clear policy as to what information should be kept on the equipment and for what purpose. Personal information is not defined in the question as the data that were lost. Insurance may be a relatively smaller issue as compared with information theft or opportunity loss, although insurance is also an important factor for a successful business. Cost of equipment would be a less important issue as compared with other choices.

**NEW QUESTION 124**

An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

- A. threat
- B. loss
- C. vulnerability
- D. probability

**Answer: C**

**Explanation:**

Implementing more restrictive preventive controls mitigates vulnerabilities but not the threats. Losses and probability of occurrence may not be primarily or directly affected.

**NEW QUESTION 126**

Phishing is BEST mitigated by which of the following?

- A. Security monitoring software
- B. Encryption
- C. Two-factor authentication
- D. User awareness

**Answer:** D

**Explanation:**

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.

#### NEW QUESTION 129

The security responsibility of data custodians in an organization will include:

- A. assuming overall protection of information asset
- B. determining data classification level
- C. implementing security controls in products they instal
- D. ensuring security measures are consistent with polic

**Answer:** D

**Explanation:**

Security responsibilities of data custodians within an organization include ensuring that appropriate security measures are maintained and are consistent with organizational policy. Executive management holds overall responsibility for protection of the information assets. Data owners determine data classification levels for information assets so that appropriate levels of controls can be provided to meet the requirements relating to confidentiality, integrity and availability. Implementation of information security in products is the responsibility of the IT developers.

#### NEW QUESTION 131

Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

- A. Number of controls implemented
- B. Percent of control objectives accomplished
- C. Percent of compliance with the security policy
- D. Reduction in the number of reported security incidents

**Answer:** B

**Explanation:**

Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

#### NEW QUESTION 135

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 139

A successful risk management program should lead to:

- A. optimization of risk reduction efforts against cos
- B. containment of losses to an annual budgeted amoun
- C. identification and removal of all man-made threat
- 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 144

A risk management program would be expected to:

- A. remove all inherent risk
- B. maintain residual risk at an acceptable level
- C. implement preventive controls for every threat
- D. reduce control risk to zero

**Answer: B**

#### Explanation:

The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

#### NEW QUESTION 145

When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

- A. the information security steering committee
- B. customers who may be impacted
- C. data owners who may be impacted
- D. regulatory agencies overseeing privacy

**Answer: C**

#### Explanation:

The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

#### NEW QUESTION 146

Which of the following would be the MOST relevant factor when defining the information classification policy?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 150

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 151

The MOST important function of a risk management program is to:

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 152

A risk mitigation report would include recommendations for:

- A. assessmen
- B. acceptance
- C. evaluatio
- D. quantificatio

**Answer: B**

#### Explanation:

Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment, evaluation and risk quantification are components of the risk analysis process that are completed prior to determining risk mitigation solutions.

#### NEW QUESTION 154

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

- A. perform a comprehensive assessment of the organization's exposure to the hacker's technique
- B. initiate awareness training to counter social engineerin
- C. immediately advise senior management of the elevated ris
- D. increase monitoring activities to provide early detection of intrusio

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 158

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 160

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 161

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

- A. Conducting a qualitative and quantitative risk analysi
- B. Assigning value to the asset
- C. Weighing the cost of implementing the plan v
- D. financial los
- E. Conducting a business impact analysis (BIA).

**Answer: D**

#### Explanation:

BIA is an essential component of an organization's business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning

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

#### NEW QUESTION 162

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

- A. transferre
- B. treat
- C. accept
- D. terminate

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 164

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 165

A risk analysis should:

- A. include a benchmark of similar companies in its scop
- B. assume an equal degree of protection for all asset
- C. address the potential size and likelihood of los
- D. give more weight to the likelihood v
- E. the size of the los

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 166

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- A. ensure the provider is made liable for losse
- B. recommend not renewing the contract upon expiratio
- C. recommend the immediate termination of the contrac
- D. determine the current level of securit

**Answer: D**

#### Explanation:

It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

#### NEW QUESTION 171

An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

- A. mitigate the impact by purchasing insuranc
- B. implement a circuit-level firewall to protect the networ
- C. increase the resiliency of security measures in plac
- D. implement a real-time intrusion detection syste

**Answer:** A

**Explanation:**

Since residual risk will always be too high, the only practical solution is to mitigate the financial impact by purchasing insurance.

**NEW QUESTION 176**

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 178**

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 182**

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 187**

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 191**

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 194**

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

- A. operations are too busy to compl
- B. the risk is justified by the benefi
- C. policy compliance would be difficult to enforc
- D. users may initially be inconvenience

**Answer:** B

**Explanation:**

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

**NEW QUESTION 195**

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

- A. Justification of the security budget must be continually mad
- B. New vulnerabilities are discovered every da
- C. The risk environment is constantly changin
- D. Management needs to be continually informed about emerging risk

**Answer:** C

**Explanation:**

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

**NEW QUESTION 197**

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

- A. policy developmen
- B. change managemen
- C. awareness trainin
- D. regular monitorin

**Answer:** B

**Explanation:**

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

**NEW QUESTION 200**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 202**

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 part 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 204

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 209

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 standard
- D. ensure that the information security expectations are conveyed to employee

**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 212

What is the BEST technique to determine which security controls to implement with a limited budget?

- A. Risk analysis
- B. Annualized loss expectancy (ALE) calculations
- C. Cost-benefit analysis
- D. Impact analysis

**Answer:** C

**Explanation:**

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

#### NEW QUESTION 216

Which of the following would BEST address the risk of data leakage?

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

**Answer:** C

**Explanation:**

Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

#### NEW QUESTION 218

When residual risk is minimized:

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 220

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 225

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 227

An information security manager uses security metrics to measure the:

- A. performance of the information security program
- B. performance of the security baseline
- C. effectiveness of the security risk analysis
- D. effectiveness of the incident response team

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 230

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

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

**Answer:** B

#### Explanation:

Percentage of unresolved risk exposures and the number of security incidents identified contribute to the IT risk management process, but the percentage of

critical assets with budgeted remedial is the most indicative metric. Number of risk management action plans is not useful for assessing the quality of the process.

#### NEW QUESTION 231

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 236

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 240

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 241

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 245

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 248

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 252

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 256

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

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

**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 258

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 262

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 264**

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 268**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 272**

Security monitoring mechanisms should PRIMARILY:

- A. focus on business-critical informatio
- B. assist owners to manage control risk
- C. focus on detecting network intrusion
- D. record all security violation

**Answer:** A

**Explanation:**

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

**NEW QUESTION 276**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 277**

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 279

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

- A. an adequate budget for the security progra
- B. recruitment of technical IT employee
- C. periodic risk assessment
- D. security awareness training for employee

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 280

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 285

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 289

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 294

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 296

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

- A. Regularly updated signature files
- B. A properly configured firewall
- C. An intrusion detection system
- D. Strict controls on input fields

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 301

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 302

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 305

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 308

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 312

An extranet server should be placed:

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 315

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

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

**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 317

Nonrepudiation can BEST be ensured by using:

- A. strong password
- B. a digital hash
- C. symmetric encryption
- 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 318

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

- A. data encryption
- B. digital signature
- C. strong password
- D. two-factor authentication

**Answer:**

D

**Explanation:**

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

**NEW QUESTION 319**

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 321**

On which of the following should a firewall be placed?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 322**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 324**

An intrusion detection system should be placed:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 325**

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

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

D. Multiple encryption algorithms

**Answer:** A

**Explanation:**

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

**NEW QUESTION 327**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 329**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 334**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 337**

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

- A. Symmetric cryptography
- B. Public key infrastructure (PKI)
- C. Message hashing
- D. Message authentication code

**Answer:** B

**Explanation:**

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

**NEW QUESTION 338**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 343**

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 logo
- B. periodic security-related e-mail message
- C. an Intranet web site for information security
- D. circulating the information security policy

**Answer:** A

**Explanation:**

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

**NEW QUESTION 346**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 351**

An intranet server should generally be placed on the:

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

**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 356**

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 357

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

- A. references from other organization
- B. past experience of the engagement team
- C. sample deliverables
- D. methodology used in the assessment

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 362

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 364

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 369

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

- A. Explicitly refer to contractors in the security standards
- B. Have the contractors acknowledge in writing the security policies
- C. Create penalties for noncompliance in the contracting agreement
- D. Perform periodic security reviews of the contractors

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 373

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 374**

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 378**

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 383**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 384**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 386**

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

- A. delegating authority to data custodians
- B. cloning existing user accounts
- C. determining hierarchical preference
- D. mapping to business need

**Answer: D**

**Explanation:**

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

**NEW QUESTION 389**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 393**

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 394**

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 399**

Information security policies should:

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

**Answer:** C

**Explanation:**

As high-level statements, information security policies should be straightforward and easy to understand. They are 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 401**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 405**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 406**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 411**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 412**

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 413**

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

- A. Perform periodic penetration testing

- B. Establish minimum security baselines
- C. Implement vendor default settings
- D. Install a honeypot on the network

**Answer:** D

**Explanation:**

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

**NEW QUESTION 416**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 420**

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 422**

An information security program should focus on:

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

**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 424**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 426**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 427**

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 429**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 431**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CISM Practice Exam Features:

- \* CISM Questions and Answers Updated Frequently
- \* CISM Practice Questions Verified by Expert Senior Certified Staff
- \* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The CISM Practice Test Here](#)