# Isaca

## Exam Questions CISM

Certified Information Security Manager

**NEW QUESTION 1**
When personal information is transmitted across networks, there MUST be adequate controls over:

A. change managemen
B. privacy protectio
C. consent to data transfe
D. encryption device

**Answer:** B

**Explanation:**

Privacy protection is necessary to ensure that the receiving party has the appropriate level of protection of personal data. Change management primarily protects only the information, not the privacy of the individuals. Consent is one of the protections that is frequently, but not always, required. Encryption is a method of achieving the actual control, but controls over the devices may not ensure adequate privacy protection and. therefore, is a partial answer.

**NEW QUESTION 2**
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 3**
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 4**
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the
Information security program?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 5**
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 (' 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 6**
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

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

**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 (KRD setup is a tool to be used in internal control assessment. KRI setup
presents a threshold to alert management when controls are being compromised in business processes. This is a control tool rather than a maturity model support tool.

**NEW QUESTION 7**
Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 8**
Which of the following is the MOST important to keep in mind when assessing the value of information?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**
Which of the following is the MOST important prerequisite for establishing information security management within an organization?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**
Which of the following is a benefit of information security governance?

A. Reduction of the potential for civil or legal liability
B. Questioning trust in vendor relationships
C. Increasing the risk of decisions based on incomplete management information
D. Direct involvement of senior management in developing control processes

**Answer:** A

**Explanation:**

Information security governance decreases the risk of civil or legal liability. The remaining answers are incorrect. Option D appears to be correct, but senior management would provide oversight and approval as opposed to direct involvement in developing control processes.

**NEW QUESTION 10**
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 12**
Which of the following is the MOST important element of an information security strategy?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 17**
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 19**
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 20**
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

A. Laws and regulations of the country of origin may not be enforceable in the foreign countr
B. A security breach notification might get delayed due to the time differenc
C. Additional network intrusion detection sensors should be installed, resulting in an additional cos
D. The company could lose physical control over the server and be unable to monitor the physical security posture of the server

**Answer:** A

**Explanation:**

A company is held to the local laws and regulations of the country in which the company resides, even if the company decides to place servers with a vendor that hosts the servers in a foreign country. A potential violation of local laws applicable to the company might not be recognized or rectified (i.e., prosecuted) due to the lack of knowledge of the local laws that are applicable and the inability to enforce the laws. Option B is not a problem. Time difference does not play a role in a 24/7 environment. Pagers, cellular phones, telephones, etc. are usually available to communicate notifications. Option C is a manageable problem that requires additional funding, but can be addressed. Option D is a problem that can be addressed. Most hosting providers have standardized the level of physical security that is in place. Regular physical audits or a SAS 70 report can address such concerns.

**NEW QUESTION 21**
At what stage of the applications development process should the security department initially become involved?

A. When requested
B. At testing
C. At programming
D. At detail requirements

**Answer:** D

**Explanation:**

Information security has to be integrated into the requirements of the application's design. It should also be part of the information security governance of the organization. The application owner may not make a timely request for security involvement. It is too late during systems testing, since the requirements have already been agreed upon. Code reviews are part of the final quality assurance process.

**NEW QUESTION 23**
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 26**
When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

A. Create separate policies to address each regulation
B. Develop policies that meet all mandated requirements
C. Incorporate policy statements provided by regulators
D. Develop a compliance risk assessment

**Answer:** B

**Explanation:**

It will be much more efficient to craft all relevant requirements into policies than to create separate versions. Using statements provided by regulators will not capture all of the requirements mandated by different regulators. A compliance risk assessment is an important tool to verify that procedures ensure compliance once the policies have been established.

**NEW QUESTION 30**
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 35**
Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

A. Chief security officer (CSO)
B. Chief operating officer (COO)
C. Chief privacy officer (CPO)
D. Chief legal counsel (CLC)

**Answer:** B

**Explanation:**

The chief operating officer (COO) is most knowledgeable of business operations and objectives. The chief privacy officer (CPO) and the chief legal counsel (CLC) may not have the knowledge of the day- to-day business operations to ensure proper guidance, although they have the same influence within the organization as the COO. Although the chief security officer (CSO) is knowledgeable of what is needed, the sponsor for this task should be someone with far-reaching influence across the organization.

**NEW QUESTION 39**
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

A. corporate data privacy polic
B. data privacy policy where data are collecte
C. data privacy policy of the headquarters' countr
D. data privacy directive applicable globall

**Answer:** B

**Explanation:**

As a subsidiary, the local entity will have to comply with the local law for data collected in the country. Senior management will be accountable for this legal compliance. The policy, being internal, cannot supersede the local law. Additionally, with local regulations differing from the country in which the organization is headquartered, it is improbable that a group wide policy will address all the local legal requirements. In case of data collected locally (and potentially transferred to a country with a different data privacy regulation), the local law applies, not the law applicable to the head office. The data privacy laws are country-specific.

**NEW QUESTION 44**
Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 45**
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions
C. Organization chart
D. Skills inventory

**Answer:** D

**Explanation:**

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

**NEW QUESTION 50**
The MOST important component of a privacy policy is:

A. notification
B. warrantie
C. liabilitie
D. geographic coverag

**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 55**
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 57**
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 62**
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 63**
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 67**
Who should drive the risk analysis for an organization?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 71**
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 organizatio
B. formulation of policies and procedures for information securit
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 76**
When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

A. Evaluate productivity losses
B. Assess the impact of confidential data disclosure
C. Calculate the value of the information or asset
D. Measure the probability of occurrence of each threat

**Answer:** C

**Explanation:**

Calculating the value of the information or asset is the first step in a risk analysis process to determine the impact to the organization, which is the ultimate goal. Determining how much productivity could be lost and how much it would cost is a step in the estimation of potential risk process. Knowing the impact if confidential information is disclosed is also a step in the estimation of potential risk. Measuring the probability of occurrence for each threat identified is a step in performing a threat analysis and therefore a partial answer.

**NEW QUESTION 77**
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 78**
Which of the following would a security manager establish to determine the target for restoration of normal processing?

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

**Answer:** A

**Explanation:**

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

required in reduced mode.

**NEW QUESTION 80**
The value of information assets is BEST determined by:

A. individual business manager
B. business systems analyst
C. information security managemen
D. industry averages benchmarkin

**Answer:** A

**Explanation:**

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

**NEW QUESTION 81**
When performing an information risk analysis, an information security manager should FIRST:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 84**
Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

A. Strategic business plan
B. Upcoming financial results
C. Customer personal information
D. Previous financial results

**Answer:** D

**Explanation:**

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

**NEW QUESTION 89**
Which of the following steps in conducting a risk assessment should be performed FIRST?

A. Identity business assets
B. Identify business risks
C. Assess vulnerabilities
D. Evaluate key controls

**Answer:** A

**Explanation:**

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

**NEW QUESTION 91**
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

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

**Answer:** A

**Explanation:**

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer

portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

**NEW QUESTION 93**
The MOST important function of a risk management program is to:

A. quantify overall ris
B. minimize residual ris
C. eliminate inherent ris
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 98**
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 103**
A company's mail server allows anonymous file transfer protocol (FTP) access which could
be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

A. A penetration test
B. A security baseline review
C. A risk assessment
D. A business impact analysis (BIA)

**Answer:** C

**Explanation:**

A risk assessment will identify- the business impact of such vulnerability being exploited and is, thus, the correct process. A penetration test or a security baseline review may identify the vulnerability but not the remedy. A business impact analysis (BIA) will more likely identify the impact of the loss of the mail server.

**NEW QUESTION 104**
Which of the following measures would be MOST effective against insider threats to confidential information?

A. Role-based access control
B. Audit trail monitoring
C. Privacy policy
D. Defense-in-depth

**Answer:** A

**Explanation:**

Role-based access control provides access according to business needs; therefore, it reduces unnecessary- access rights and enforces accountability. Audit trail monitoring is a detective control, which is 'after the fact.' Privacy policy is not relevant to this risk. Defense-in-depth primarily focuses on external threats

**NEW QUESTION 109**
Which of the following results from the risk assessment process would BEST assist risk management decision making?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 113**
Which of the following would generally have the GREATEST negative impact on an organization?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 114**
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 119**
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

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

**Answer:** A

**Explanation:**

In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control. Frequent risk assessment programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will contribute to the value of the risk but. alone, will not justify a control.

**NEW QUESTION 123**
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 127**
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 130**
The PRIMARY objective of a risk management program is to:

A. minimize inherent ris
B. eliminate business ris
C. implement effective control
D. minimize residual ris

**Answer:** D

**Explanation:**

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

**NEW QUESTION 135**
A risk management program should reduce risk to:

A. zer
B. an acceptable leve
C. an acceptable percent of revenu
D. an acceptable probability of occurrenc

**Answer:** B

**Explanation:**

Risk should be reduced to an acceptable level based on the risk preference of the organization. Reducing risk to zero is impractical and could be cost-prohibitive. Tying risk to a percentage of revenue is inadvisable since there is no direct correlation between the two. Reducing the probability of risk occurrence may not always be possible, as in the ease of natural disasters. The focus should be on reducing the impact to an acceptable level to the organization, not reducing the probability of the risk.

**NEW QUESTION 139**
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

A. conduct a risk assessment and allow or disallow based on the outcom
B. recommend a risk assessment and implementation only if the residual risks are accepte
C. recommend against implementation because it violates the company's policie
D. recommend revision of current polic

**Answer:** B

**Explanation:**

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

**NEW QUESTION 140**
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 144**

Who is responsible for ensuring that information is classified?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 146**
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

A. IT assets in key business functions are protecte
B. business risks are addressed by preventive control
C. stated objectives are achievabl
D. IT facilities and systems are always availabl

**Answer:** C

**Explanation:**

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

**NEW QUESTION 149**
When performing a risk assessment, the MOST important consideration is that:

A. management supports risk mitigation effort
B. annual loss expectations (ALEs) have been calculated for critical asset
C. assets have been identified and appropriately value
D. attack motives, means and opportunities be understoo

**Answer:** C

**Explanation:**

Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. ALE calculations are only valid if assets have first been identified and appropriately valued. Motives, means and opportunities should already be factored in as a part of a risk assessment.

**NEW QUESTION 151**
Which of the following risks is represented in the risk appetite of an organization?

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

**Answer:** C

**Explanation:**

Residual risk is unmanaged, i.e., inherent risk which remains uncontrolled. This is key to the organization's risk appetite and is the amount of residual risk that a business is living with that affects its viability. Hence, inherent risk is incorrect. Control risk, the potential for controls to fail, and audit risk, which relates only to audit's approach to their work, are not relevant in this context.

**NEW QUESTION 154**
Which two components PRIMARILY must be assessed in an effective risk analysis?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 159**
Identification and prioritization of business risk enables project managers to:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 162**
Which of the following is the MOST appropriate use of gap analysis?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 165**
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 166**
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 170**
Which of the following guarantees that data in a file have not changed?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 174**
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 177**
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 180**
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 181**
Which of the following is the MOST effective type of access control?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 185**
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 188**
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 191**
To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A. revise the information security progra
B. evaluate a balanced business scorecar
C. conduct regular user awareness session
D. perform penetration test

**Answer:** B

**Explanation:**

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

**NEW QUESTION 195**
An intrusion detection system should be placed:

A. outside the firewal
B. on the firewall serve
C. on a screened subne
D. on the external route

**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 tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical dcvice.

**NEW QUESTION 198**
When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

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

**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 203**
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. Eocus 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 206**
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

A. contribute cost-effective expertise not available internall
B. be made responsible for meeting the security program requirement
C. replace the dependence on internal resource
D. deliver more effectively on account of their knowledg

**Answer:** A

**Explanation:**

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

**NEW QUESTION 208**
Secure customer use of an e-commerce application can BEST be accomplished through:

A. data encryptio
B. digital signature
C. strong password
D. two-factor authenticatio

**Answer:** A

**Explanation:**

Encryption would be the preferred method of ensuring confidentiality in customer communications with an e-commerce application. Strong passwords, by themselves, would not be sufficient since the data could still be intercepted, while two-factor authentication would be impractical. Digital signatures would not provide a secure means of communication. In most business-to-customer (B-to-C) web applications, a digital signature is also not a practical solution.

**NEW QUESTION 212**
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 215**
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

A. the parties to the agreement can perfor
B. confidential data are not included in the agreemen
C. appropriate controls are include
D. the right to audit is a requiremen

**Answer:** C

**Explanation:**

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

**NEW QUESTION 218**
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 221**
The PRIMARY objective of an Internet usage policy is to prevent:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 225**
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 repor
B. Conduct a penetration tes
C. Obtain approval from senior managemen
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 228**
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

A. System monitoring for traffic on network ports
B. Security code reviews for the entire application
C. Reverse engineering the application binaries
D. Running the application from a high-privileged account on a test system

**Answer:** B

**Explanation:**

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

**NEW QUESTION 232**
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

A. the existence of messages is unknow
B. required key sizes are smalle
C. traffic cannot be sniffe
D. reliability of the data is higher in transi

**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 236**
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 239**
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 244**
In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 248**
Data owners will determine what access and authorizations users will have by:

A. delegating authority to data custodia
B. cloning existing user account
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 249**
To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

A. end user
B. legal counse
C. operational unit
D. audit managemen

**Answer:** C

**Explanation:**

Procedures at the operational level must be developed by or with the involvement of operational units that will use them. This will ensure that they are functional and accurate. End users and legal counsel are normally not involved in procedure development. Audit management generally oversees information security operations but does not get involved at the procedural level.

**NEW QUESTION 250**
To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

A. set their accounts to expire in six months or les
B. avoid granting system administration role

C. ensure they successfully pass background check
D. ensure their access is approved by the data owne

**Answer:** B

**Explanation:**

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

**NEW QUESTION 254**
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 259**
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 263**
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 264**
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 268**
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 273**
Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 276**
What is the MOST important element to include when developing user security awareness material?

A. Information regarding social engineering
B. Detailed security policies
C. Senior management endorsement
D. Easy-to-read and compelling information

**Answer:** D

**Explanation:**

Making security awareness material easy and compelling to read is the most important success factor. Users must be able to understand, in easy terms, complex security concepts in a way that makes compliance more accessible. Choice A would also be important but it needs to be presented in an adequate format. Detailed security policies might not necessarily be included in the training materials. Senior management endorsement is important for the security program as a whole and not necessarily for the awareness training material.

**NEW QUESTION 278**
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 282**
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 286**
Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A. Acceptable use policy
B. Setting low mailbox limits
C. User awareness training
D. Taking disciplinary action

**Answer:** C

**Explanation:**

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

**NEW QUESTION 291**
In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 294**
What is the GREATEST risk when there is an excessive number of firewall rules?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 298**
What is the BEST method to verify that all security patches applied to servers were properly documented?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 301**
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

A. Attempt to reset several passwords to weaker values
B. Install code to capture passwords for periodic audit
C. Sample a subset of users and request their passwords for review
D. Review general security settings on each platform

**Answer:** D

**Explanation:**

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

**NEW QUESTION 304**
Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

A. are compatible with the provider's own classificatio
B. are communicated to the provide
C. exceed those of the outsource
D. are stated in the contrac

**Answer:** D

**Explanation:**

The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A. B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

**NEW QUESTION 305**
What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

A. Provide detailed instructions on how to carry out different types of tasks
B. Ensure consistency of activities to provide a more stable environment
C. Ensure compliance to security standards and regulatory requirements
D. Ensure reusability to meet compliance to quality requirements

**Answer:** B

**Explanation:**

Developing procedures and guidelines to ensure that business processes address information security risk is critical to the management of an information security program. Developing procedures and guidelines establishes a baseline for security program performance and consistency of security activities.

**NEW QUESTION 310**
When security policies are strictly enforced, the initial impact is that:

A. they may have to be modified more frequentl
B. they will be less subject to challeng
C. the total cost of security is increase
D. the need for compliance reviews is decrease

**Answer:** C

**Explanation:**

When security policies are strictly enforced, more resources are initially required, thereby increasing, the total cost of security. There would be less need for frequent modification. Challenges would be rare and the need for compliance reviews would not necessarily be less.

**NEW QUESTION 314**
Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

A. Information security officer
B. Security steering committee
C. Data owner
D. Data custodian

**Answer:** B

**Explanation:**

Routine administration of all aspects of security is delegated, but senior management must retain overall responsibility. The information security officer supports and implements information security for senior management. The data owner is responsible for categorizing data security requirements. The data custodian supports and implements information security as directed.

**NEW QUESTION 319**
Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 320**
A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

A. Enable access through a separate device that requires adequate authentication
B. Implement manual procedures that require password change after each use
C. Request the vendor to add multiple user IDs
D. Analyze the logs to detect unauthorized access

**Answer:** A

**Explanation:**

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual.
Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but. because it is detective, it would not be the most effective in this instance.

**NEW QUESTION 323**
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testin
B. establish security baseline
C. implement vendor default setting
D. link policies to an independent standar

**Answer:** B

**Explanation:**

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

**NEW QUESTION 326**
The BEST way to ensure that information security policies are followed is to:

A. distribute printed copies to all employee
B. perform periodic reviews for complianc
C. include escalating penalties for noncomplianc
D. establish an anonymous hotline to report policy abuse

**Answer:** B

**Explanation:**

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

**NEW QUESTION 328**
A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 329**
Which of the following is the FIRST phase in which security should be addressed in the development cycle of a project?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 331**
In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

A. volume of sensitive dat
B. recovery point objective (RPO).
C. recovery' time objective (RTO).
D. interruption windo

**Answer:** B

**Explanation:**

The recovery point objective (RPO) defines the maximum loss of data (in terms of time) acceptable by the business (i.e., age of data to be restored). It will directly determine the basic elements of the backup strategy frequency of the backups and what kind of backup is the most appropriate (disk-to-disk, on tape, mirroring). The volume of data will be used to determine the capacity of the backup solution. The recovery time objective (RTO)—the time between disaster and return to normal operation—will not have any impact on the backup strategy. The availability to restore backups in a time frame consistent with the interruption window will have to be checked and will influence the strategy (e.g., full backup vs. incremental), but this will not be the primary factor.

**NEW QUESTION 332**
Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m. (23.00 hrs.)?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 337**
If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A. obtaining evidence as soon as possibl
B. preserving the integrity of the evidenc
C. disconnecting all IT equipment involve
D. reconstructing the sequence of event

**Answer:** B

**Explanation:**

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

**NEW QUESTION 339**
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

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

**Answer:** A

**Explanation:**

A business impact analysis (BIA) provides results, such as impact from a security incident and required response times. The BIA is the most critical process for deciding which part of the information system/ business process should be given prioritization in case of a security incident. Risk assessment is a very important process for the creation of a business continuity plan. Risk assessment provides information on the likelihood of occurrence of security incidence and assists in the

selection of countermeasures. but not in the prioritization. As in choice B, a vulnerability assessment provides information regarding the security weaknesses of the system, supporting the risk analysis process. Business process mapping facilitates the creation of the plan by providing mapping guidance on actions after the decision on critical business processes has been made-translating business prioritization to IT prioritization. Business process mapping does not help in making a decision, but in implementing a decision.

**NEW QUESTION 343**
Which of the following actions should lake place immediately after a security breach is reported to an information security manager?

A. Confirm the incident
B. Determine impact
C. Notify affected stakeholders
D. Isolate the incident

**Answer:** A

**Explanation:**

Before performing analysis of impact, resolution, notification or isolation of an incident, ii must be validated as a real security incident.

**NEW QUESTION 348**
The FIRST priority when responding to a major security incident is:

A. documentatio
B. monitorin
C. restoratio
D. containmen

**Answer:** D

**Explanation:**

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

**NEW QUESTION 350**
A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 352**
An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

A. Unsure that critical data on the server are backed u
B. Shut down the compromised serve
C. Initiate the incident response proces
D. Shut down the networ

**Answer:** C

**Explanation:**

The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

**NEW QUESTION 353**
To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

A. Database server
B. Domain name server (DNS)
C. Time server
D. Proxy server

**Answer:** C

**Explanation:**

To accurately reconstruct the course of events, a time reference is needed and that is provided by the time server. The other choices would not assist in the correlation and review1 of these logs.

**NEW QUESTION 356**
Which of the following application systems should have the shortest recovery time objective (RTO)?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 360**
Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 361**
Which of the following is MOST important in determining whether a disaster recovery test is successful?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 362**
The PRIMARY purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

A. weaknesses in network and server securit
B. ways to improve the incident response proces
C. potential attack vectors on the network perimete
D. the optimum response to internal hacker attack

**Answer:** A

**Explanation:**

An internal attack and penetration test are designed to identify weaknesses in network and server security. They do not focus as much on incident response or the network perimeter.

**NEW QUESTION 366**
Detailed business continuity plans should be based PRIMARILY on:

A. consideration of different alternative
B. the solution that is least expensiv
C. strategies that cover all application
D. strategies validated by senior managemen

**Answer:** D

**Explanation:**

A recovery strategy identifies the best way to recover a system in ease of disaster and provides guidance based on detailed recovery procedures that can be developed. Different strategies should be developed and all alternatives presented to senior management. Senior management should select the most appropriate strategy from the alternatives provided. The selected strategy should be used for further development of the detailed business continuity plan. The selection of strategy depends on criticality of the business process and applications supporting the processes. It need not necessarily cover all applications. All recovery strategies have associated costs, which include costs of preparing for disruptions and putting them to use in the event of a disruption. The latter can be insured against, but not the former. The best recovery option need not be the least expensive.

**NEW QUESTION 369**
The business continuity policy should contain which of the following?

A. Emergency call trees
B. Recovery criteria
C. Business impact assessment (BIA)
D. Critical backups inventory

**Answer:** B

**Explanation:**

Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

**NEW QUESTION 372**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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