



**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 management
- B. privacy protection
- C. consent to data transfer
- 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

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 3

The FIRST step in establishing a security governance program is to:

- A. conduct a risk assessment
- B. conduct a workshop for all end user
- C. prepare a security budget
- D. obtain high-level sponsorship

**Answer: D**

#### Explanation:

The establishment of a security governance program is possible only with the support and sponsorship of top management since security governance projects are enterprise wide and integrated into business processes. Conducting a risk assessment, conducting a workshop for all end users and preparing a security budget all follow once high-level sponsorship is obtained.

#### NEW QUESTION 4

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 5

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 6**

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 7**

Investments in information security technologies should be based on:

- A. vulnerability assessment
- B. value analysi
- C. business climat
- D. audit recommendation

**Answer:** B

**Explanation:**

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

**NEW QUESTION 8**

Information security governance is PRIMARILY driven by:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 9**

The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

- A. head of internal audi
- B. chief operations officer (COO).
- C. chief technology officer (CTO).
- D. legal counse

**Answer:** B

**Explanation:**

The chief information security officer (CISO) should ideally report to as high a level within the organization as possible. Among the choices given, the chief operations officer (COO) would have not only the appropriate level but also the knowledge of day-to-day operations. The head of internal audit and legal counsel would make good secondary choices, although they would not be as knowledgeable of the operations. Reporting to the chief technology officer (CTO) could become problematic as the CTO's goals for the infrastructure might, at times, run counter to the goals of information security.

**NEW QUESTION 10**

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

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

D. aligned with the business strateg

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 10

Information security policy enforcement is the responsibility of the:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 11

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 16

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

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

**Answer:** B

**Explanation:**

Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

#### NEW QUESTION 21

Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

- A. organizational ris
- B. organization wide metric
- C. security need
- D. the responsibilities of organizational unit

**Answer:** A

**Explanation:**

Information security exists to help the organization meet its objectives. The information security manager should identify information security needs based on organizational needs. Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior management after the overall organizational risk is identified.

#### NEW QUESTION 26

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 27**

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 31**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 33**

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

- A. ability to mitigate business risk
- B. evaluations in trade publication
- C. use of new and emerging technologie
- D. benefits in comparison to their cost

**Answer:** A

**Explanation:**

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

**NEW QUESTION 37**

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 40**

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 44**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 45**

Who is ultimately responsible for the organization's information?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 48**

Retention of business records should PRIMARILY be based on:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 50**

What is the MOST important factor in the successful implementation of an enterprise wide information security program?

- A. Realistic budget estimates
- B. Security awareness
- C. Support of senior management
- D. Recalculation of the work factor

**Answer:** C

**Explanation:**

Without the support of senior management, an information security program has little chance of survival. A company's leadership group, more than any other group, will more successfully drive the program. Their authoritative position in the company is a key factor. Budget approval, resource commitments, and companywide participation also require the buy-in from senior management. Senior management is responsible for providing an adequate budget and the necessary resources. Security awareness is important, but not the most important factor. Recalculation of the work factor is a part of risk management.



#### NEW QUESTION 52

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

- A. a statement regarding what the company will do with the information it collect
- B. a disclaimer regarding the accuracy of information on its web sit
- C. technical information regarding how information is protecte
- D. a statement regarding where the information is being hoste

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 55

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 59

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

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

**Answer:** B

#### Explanation:

Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

#### NEW QUESTION 60

To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

- A. Security breach frequency
- B. Annualized loss expectancy (ALE)
- C. Cost-benefit analysis
- D. Peer group comparison

**Answer:** C

#### Explanation:

Cost-benefit analysis is the legitimate way to justify budget. The frequency of security breaches may assist the argument for budget but is not the key tool; it does not address the impact. Annualized loss expectancy (ALE) does not address the potential benefit of security investment. Peer group comparison would provide a good estimate for the necessary security budget but it would not take into account the specific needs of the organization.

#### NEW QUESTION 63

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

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

**Answer:** B

#### Explanation:

New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support.

Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

#### NEW QUESTION 65

Information security should be:

- A. focused on eliminating all risk
- B. a balance between technical and business requirement
- C. driven by regulatory requirement
- D. defined by the board of director

**Answer: B**

#### Explanation:

Information security should ensure that business objectives are met given available technical capabilities, resource constraints and compliance requirements. It is not practical or feasible to eliminate all risks. Regulatory requirements must be considered, but are inputs to the business considerations. The board of directors does not define information security, but provides direction in support of the business goals and objectives.

#### NEW QUESTION 67

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 69

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 72

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 73

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

- A. return on investment (RO
- B. a vulnerability assessmen
- C. annual loss expectancy (ALE).
- D. a business cas

**Answer: D**

#### Explanation:



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

#### NEW QUESTION 76

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 81

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 83

The cost of implementing a security control should not exceed the:

- A. annualized loss expectancy
- B. cost of an incident
- C. asset value
- D. implementation opportunity cost

**Answer: C**

#### Explanation:

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses that are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

#### NEW QUESTION 87

The value of information assets is BEST determined by:

- A. individual business manager
- B. business systems analyst
- C. information security management
- D. industry averages benchmarking

**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 90

The BEST strategy for risk management is to:

- A. achieve a balance between risk and organizational goal
- B. reduce risk to an acceptable level

- C. ensure that policy development properly considers organizational risk
- D. ensure that all unmitigated risks are accepted by management

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 92

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 inventory
- D. categorize the asset

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 95

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 97

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 101

Previously accepted risk should be:

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 103

Phishing is BEST mitigated by which of the following?

- A. Security monitoring software

- B. Encryption
- C. Two-factor authentication
- D. User awareness

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 106

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 107

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 112

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

- A. Feasibility
- B. Design
- C. Development
- D. Testing

**Answer:** A

**Explanation:**

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

#### NEW QUESTION 113

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 118

Which program element should be implemented FIRST in asset classification and control?

- A. Risk assessment

- B. Classification
- C. Valuation
- D. Risk mitigation

**Answer:** C

**Explanation:**

Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

#### NEW QUESTION 123

An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

- A. Nothing, since a risk assessment was completed during developmen
- B. A vulnerability assessment should be conducte
- C. A new risk assessment should be performe
- D. The new vendor's SAS 70 type II report should be reviewe

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 126

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

- A. original cost to acquire
- B. cost of the software store
- C. annualized loss expectancy (ALE).
- D. cost to obtain a replacemen

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 129

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 133

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 135

The MAIN reason why asset classification is important to a successful information security program is because classification determines:

- A. the priority and extent of risk mitigation effort
- B. the amount of insurance needed in case of loss
- C. the appropriate level of protection to the asset
- D. how protection levels compare to peer organization

**Answer:** C

**Explanation:**

Protection should be proportional to the value of the asset. Classification is based upon the value of the asset to the organization. The amount of insurance needed in case of loss may not be applicable in each case. Peer organizations may have different classification schemes for their assets.

#### NEW QUESTION 137

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 142

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

- A. Platform security
- B. Entitlement changes
- C. Intrusion detection
- D. Antivirus controls

**Answer:** B

**Explanation:**

Data owners are responsible for assigning user entitlements and approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

#### NEW QUESTION 144

A common concern with poorly written web applications is that they can allow an attacker to:

- A. gain control through a buffer overflow
- B. conduct a distributed denial of service (DoS) attack
- C. abuse a race condition
- D. inject structured query language (SQL) statement

**Answer:** D

**Explanation:**

Structured query language (SQL) injection is one of the most common and dangerous web application vulnerabilities. Buffer overflows and race conditions are very difficult to find and exploit on web applications. Distributed denial of service (DoS) attacks have nothing to do with the quality of a web application.

#### NEW QUESTION 148

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- A. Business impact analyses
- B. Security gap analyses
- C. System performance metrics
- D. Incident response processes

**Answer:** B

**Explanation:**

A security gap analysis is a process which measures all security controls in place against typically good business practice, and identifies related weaknesses. A business impact analysis is less suited to identify security deficiencies. System performance metrics may indicate security weaknesses, but that is not their primary purpose. Incident response processes exist for cases where security weaknesses are exploited.

#### NEW QUESTION 153

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

- A. Conducting a qualitative and quantitative risk analysis



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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 154

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

- A. transferre
- B. treate
- C. accepte
- D. terminate

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 157

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 162

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 164

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 166

The criticality and sensitivity of information assets is determined on the basis of:

- A. threat assessmen
- B. vulnerability assessmen
- C. resource dependency assessmen
- D. impact assessmen

**Answer:** D

#### Explanation:

The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

#### NEW QUESTION 170

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 172

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 174

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 177

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 179

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

- A. Access control policy
- B. Data classification policy
- C. Encryption standards
- D. Acceptable use policy

**Answer:** B

#### Explanation:

Data classification policies define the level of protection to be provided for each category of data. Without this mandated ranking of degree of protection, it is difficult to determine what access controls or levels of encryption should be in place. An acceptable use policy is oriented more toward the end user and, therefore, would not specifically address what controls should be in place to adequately protect information.

#### NEW QUESTION 184

There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

- A. Identify the vulnerable systems and apply compensating controls
- B. Minimize the use of vulnerable systems
- C. Communicate the vulnerability to system users
- D. Update the signatures database of the intrusion detection system (IDS)

**Answer:** A

#### Explanation:

The best protection is to identify the vulnerable systems and apply compensating controls until a patch is installed. Minimizing the use of vulnerable systems and communicating the vulnerability to system users could be compensating controls but would not be the first course of action. Choice D does not make clear the timing of when the intrusion detection system (IDS) signature list would be updated to accommodate the vulnerabilities that are not yet publicly known. Therefore, this approach should not always be considered as the first option.

#### NEW QUESTION 188

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 192

The purpose of a corrective control is to:

- A. reduce adverse event
- B. indicate compromis
- C. mitigate impac
- D. ensure complianc

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 195

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- A. Risk analysis process
- B. Business impact analysis (BIA)
- C. Risk management balanced scorecard

D. Risk-based audit program

**Answer:** B

**Explanation:**

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

#### NEW QUESTION 197

A risk management approach to information protection is:

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 198

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 203

An information security organization should PRIMARILY:

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 204

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 208

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

- A. Theft of purchased software

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 209

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 210

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 214

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 218

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

- A. corporate internal auditor
- B. System developers/analyst
- C. key business process owner
- D. corporate legal counsel

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 223

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 226

An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

- A. Rewrite the application to conform to the upgraded operating system
- B. Compensate for not installing the patch with mitigating controls
- C. Alter the patch to allow the application to run in a privileged state
- D. Run the application on a test platform; tune production to allow patch and application

**Answer:** B

**Explanation:**

Since the operating system (OS) patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security. Since the application is critical, the patch should not be applied without regard for the application; business requirements must be considered. Altering the OS patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative since it will mean running a critical production application on a platform not subject to the same level of security controls.

#### NEW QUESTION 230

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

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

**Answer:** D

**Explanation:**

The balanced scorecard is most effective for evaluating the degree to which information security objectives are being met. A SWOT analysis addresses strengths, weaknesses, opportunities and threats. Although useful, a SWOT analysis is not as effective a tool. Similarly, a gap analysis, while useful for identifying the difference between the current state and the desired future state, is not the most appropriate tool. A waterfall chart is used to understand the flow of one process into another.

#### NEW QUESTION 232

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

- A. verify the decision with the business unit
- B. check the system's risk analysis
- C. recommend update after post implementation review
- D. request an audit review

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 237

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

- A. Use security tokens for authentication
- B. Connect through an IPSec VPN
- C. Use https with a server-side certificate
- D. Enforce static media access control (MAC) addresses

**Answer:** B

**Explanation:**

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



kind of MitM attack—may be prevented by setting static media access control (MAC) addresses. Nevertheless, DNS and NetBIOS resolution can still be attacked to deviate traffic.

#### NEW QUESTION 242

A border router should be placed on which of the following?

- A. Web server
- B. IDS server
- C. Screened subnet
- D. Domain boundary

**Answer: D**

#### Explanation:

A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

#### NEW QUESTION 246

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

- A. service level monitorin
- B. penetration testin
- C. periodically auditin
- D. security awareness trainin

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 251

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 256

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 261

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

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

**Answer: C**

#### Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves



the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

#### NEW QUESTION 264

Which of the following devices should be placed within a demilitarized zone (DMZ )?

- A. Network switch
- B. Web server
- C. Database server
- D. File/print server

**Answer:** B

#### Explanation:

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

#### NEW QUESTION 268

Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

- A. Screened subnets
- B. Information classification policies and procedures
- C. Role-based access controls
- D. Intrusion detection system (IDS)

**Answer:** A

#### Explanation:

Screened subnets are demilitarized zones (DMZs) and are oriented toward preventing attacks on an internal network by external users. The policies and procedures to classify information will ultimately result in better protection but they will not prevent actual modification. Role-based access controls would help ensure that users only had access to files and systems appropriate for their job role. Intrusion detection systems (IDS) are useful to detect invalid attempts but they will not prevent attempts.

#### NEW QUESTION 272

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 277

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

- A. Configuration of firewalls
- B. Strength of encryption algorithms
- C. Authentication within application
- D. Safeguards over keys

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 279

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

- A. invite an external consultant to create the security strateg
- B. allocate budget based on best practice
- C. benchmark similar organization

D. define high-level business security requirement

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 283

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 288

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 292

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 295

The BEST metric for evaluating the effectiveness of a firewall is the:

- A. number of attacks blocke
- B. number of packets droppe
- C. average throughput rat
- D. number of firewall rule

**Answer:** A

**Explanation:**

The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not effective measurements.

#### NEW QUESTION 297

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 298

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 301

An extranet server should be placed:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 306

Nonrepudiation can BEST be ensured by using:

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 310

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 314

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 319

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 324

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 327

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 329

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

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

**Answer:**

A

**Explanation:**

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

**NEW QUESTION 333**

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

- A. critical information resources needing protectio
- B. a security policy for the entire organizatio
- C. the minimum acceptable security to be implemente
- D. required physical and logical access control

**Answer: C**

**Explanation:**

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

**NEW QUESTION 334**

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 its 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 337**

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

**NEW QUESTION 339**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 340**

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

- A. right-to-terminate claus



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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 342

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 344

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 346

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 350

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

- A. Encryption
- B. Digital certificate
- C. Digital signature
- D. Hashing algorithm

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 354

Good information security standards should:

- A. define precise and unambiguous allowable limit
- B. describe the process for communicating violation



- C. address high-level objectives of the organization
- D. be updated frequently as new software is released

**Answer:** A

**Explanation:**

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

**NEW QUESTION 356**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 360**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 361**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 363**

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 366**

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

- A. Mantrap
- B. Biometric lock
- C. Closed-circuit television (CCTV)
- D. Security guard

**Answer:** B

**Explanation:**

A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

#### NEW QUESTION 371

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 376

Good information security procedures should:

- A. define the allowable limits of behavior
- B. underline the importance of security governance
- C. describe security baselines for each platform
- D. be updated frequently as new software is released

**Answer:** D

**Explanation:**

Security procedures often have to change frequently to keep up with changes in software. Since a procedure is a how-to document, it must be kept up-to-date with frequent changes in software. A security standard such as platform baselines—defines behavioral limits, not the how-to process; it should not change frequently. High-level objectives of an organization, such as security governance, would normally be addressed in a security policy.

#### NEW QUESTION 381

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 382

Which of the following is the MOST effective, positive method to promote security awareness?

- A. Competitions and rewards for compliance
- B. Lock-out after three incorrect password attempts
- C. Strict enforcement of password formats
- D. Disciplinary action for noncompliance

**Answer:** A

**Explanation:**

Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

#### NEW QUESTION 385

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 390

In business-critical applications, user access should be approved by the:

- A. information security manager
- B. data owner
- C. data custodian
- D. business management

**Answer: B**

**Explanation:**

A data owner is in the best position to validate access rights to users due to their deep understanding of business requirements and of functional implementation within the application. This responsibility should be enforced by the policy. An information security manager will coordinate and execute the implementation of the role-based access control. A data custodian will ensure that proper safeguards are in place to protect the data from unauthorized access; it is not the data custodian's responsibility to assign access rights. Business management is not, in all cases, the owner of the data.

#### NEW QUESTION 391

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

- A. delegating authority to data custodian
- 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 393

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

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 398

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

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 403

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 408

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

- A. end user
- B. legal counsel
- C. operational unit
- D. audit management

**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 413

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 less
- B. avoid granting system administration role
- C. ensure they successfully pass background check
- D. ensure their access is approved by the data owner

**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 414

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 415

Security audit reviews should PRIMARILY:

- A. ensure that controls operate as required
- B. ensure that controls are cost-effective
- C. focus on preventive control
- D. ensure controls are technologically current

**Answer: A**

**Explanation:**

The primary objective of a security review or audit should be to provide assurance on the adequacy of security controls. Reviews should focus on all forms of control, not just on preventive control. Cost-effectiveness and technological currency are important but not as critical.

**NEW QUESTION 416**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 420**

Information security policies should:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 424**

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 426**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 428**

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

- A. Delivery path tracing



- B. Reverse lookup translation
- C. Out-of-band channels
- D. Digital signatures

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 431

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 434

An information security program should focus on:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 436

Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

- A. Database administrator (DBA )
- B. Finance department management
- C. Information security manager
- D. IT department management

**Answer:** B

**Explanation:**

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

#### NEW QUESTION 437

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 438

Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

- A. User security procedures
- B. Business process flow
- C. IT security policy
- D. Regulatory requirements

**Answer: C**

#### Explanation:

IT management should ensure that mechanisms are implemented in line with IT security policy. Procedures are determined by the policy. A user security procedure does not describe the access control mechanism in place. The business process flow is not relevant to the access control mechanism. The organization's own policy and procedures should take into account regulatory requirements.

#### NEW QUESTION 443

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 447

The BEST way to ensure that an external service provider complies with organizational security policies is to:

- A. Explicitly include the service provider in the security policies
- B. Receive acknowledgment in writing stating the provider has read all policies
- C. Cross-reference to policies in the service level agreement
- D. Perform periodic reviews of the service provider

**Answer: D**

#### Explanation:

Periodic reviews will be the most effective way of obtaining compliance from the external service provider. References in policies and service level agreements and requesting written acknowledgement will not be as effective since they will not trigger the detection of noncompliance.

#### NEW QUESTION 449

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 452

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 457

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 461

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

- A. business process owner
- B. the information security manager
- C. the security steering committee
- D. IT senior management

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 463

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 466

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

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

**Answer:** D

#### Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. The other choices are physical controls which by themselves would not be effective against tailgating.

#### NEW QUESTION 467

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

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

**Answer:**

A

**Explanation:**

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

**NEW QUESTION 469**

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 470**

Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

- A. Adequate security policies and procedures
- B. Periodic compliance reviews
- C. Security steering committees
- D. Security awareness campaigns

**Answer: D**

**Explanation:**

Security awareness campaigns will be more effective at changing an organizational culture than the creation of steering committees and security policies and procedures. Compliance reviews are helpful; however, awareness by all staff is more effective because compliance reviews are focused on certain areas groups and do not necessarily educate.

**NEW QUESTION 474**

When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

- A. submit the issue to the steering committee
- B. conduct an impact analysis to quantify the risk
- C. isolate the system from the rest of the network
- D. request a risk acceptance from senior management

**Answer: B**

**Explanation:**

An impact analysis is warranted to determine whether a risk acceptance should be granted and to demonstrate to the department the danger of deviating from the established policy. Isolating the system would not support the needs of the business. Any waiver should be granted only after performing an impact analysis.

**NEW QUESTION 476**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### CISM Practice Exam Features:

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

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