



**Isaca**

## **Exam Questions CISM**

Certified Information Security Manager

#### NEW QUESTION 1

An outcome of effective security governance is:

- A. business dependency assessment
- B. strategic alignment
- C. risk assessment
- D. planning

**Answer: B**

#### Explanation:

Business dependency assessment is a process of determining the dependency of a business on certain information resources. It is not an outcome or a product of effective security management. Strategic alignment is an outcome of effective security governance. Where there is good governance, there is likely to be strategic alignment. Risk assessment is not an outcome of effective security governance; it is a process. Planning comes at the beginning of effective security governance, and is not an outcome but a process.

#### NEW QUESTION 2

Successful implementation of information security governance will FIRST require:

- A. security awareness training
- B. updated security policies
- C. a computer incident management team
- D. a security architecture

**Answer: B**

#### Explanation:

Updated security policies are required to align management objectives with security procedures; management objectives translate into policy, policy translates into procedures. Security procedures will necessitate specialized teams such as the computer incident response and management group as well as specialized tools such as the security mechanisms that comprise the security architecture. Security awareness will promote the policies, procedures and appropriate use of the security mechanisms.

#### NEW QUESTION 3

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 4

Investments in information security technologies should be based on:

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 5

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

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

**Answer:**

B

**Explanation:**

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

**NEW QUESTION 6**

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 7**

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 8**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 9**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 10**

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 10

Which of the following is a benefit of information security governance?

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 14

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 16

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 18

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

- A. Ethics
- B. Proportionality
- C. Integration
- D. Accountability

**Answer:** B

**Explanation:**

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules (types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

#### NEW QUESTION 19

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 21

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 22

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 23

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

- A. use illustrative examples of successful attack
- B. explain the technical risks to the organization
- C. evaluate the organization against best security practice
- D. tie security risks to key business objective

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 25

Which of the following would BEST prepare an information security manager for regulatory reviews?

- A. Assign an information security administrator as regulatory liaison
- B. Perform self-assessments using regulatory guidelines and reports
- C. Assess previous regulatory reports with process owners input
- D. Ensure all regulatory inquiries are sanctioned by the legal department

**Answer:** B

**Explanation:**

Self-assessments provide the best feedback on readiness and permit identification of items requiring remediation. Directing regulators to a specific person or department, or assessing previous reports, is not as effective. The legal department should review all formal inquiries but this does not help prepare for a regulatory review.

#### NEW QUESTION 30

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 35

Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

- A. baselin
- B. strateg
- C. procedur
- D. polic

**Answer:** D

**Explanation:**

A policy is a high-level statement of an organization's beliefs, goals, roles and objectives. Baselines assume a minimum security level throughout an organization. The information security strategy aligns the information security program with business objectives rather than making control statements. A procedure is a step-by-step process of how policy and standards will be implemented.

#### NEW QUESTION 38

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 41

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 43

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

- A. Compliance with international security standard
- B. Use of a two-factor authentication syste
- C. Existence of an alternate hot site in case of business disruptio
- D. Compliance with the organization's information security requirement

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 45

The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

- A. storage capacity and shelf life
- B. regulatory and legal requirement
- C. business strategy and direction
- D. application systems and media

**Answer:** D

#### Explanation:

Long-term retention of business records may be severely impacted by changes in application systems and media. For example, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply, nor do legal and regulatory requirements. Storage capacity and shelf life are important but secondary issues.

#### NEW QUESTION 48

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 50

When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- A. information security metric
- B. knowledge required to analyze each issue
- C. linkage to business area objective
- D. baseline against which metrics are evaluated

**Answer:** C

#### Explanation:

The link to business objectives is the most important element that would be considered by management. Information security metrics should be put in the context of impact to management objectives. Although important, the security knowledge required would not be the first element to be considered. Baselining against the information security metrics will be considered later in the process.

#### NEW QUESTION 52

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 56

The data access requirements for an application should be determined by the:

- A. legal department
- B. compliance office
- C. information security manager
- D. business owner

**Answer:** D

**Explanation:**

Business owners are ultimately responsible for their applications. The legal department, compliance officer and information security manager all can advise, but do not have final responsibility.

#### NEW QUESTION 57

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 61

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 65

The MOST important component of a privacy policy is:

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 66

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 71

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 75

Who in an organization has the responsibility for classifying information?

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 78

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 79

Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

- A. The information security department has difficulty filling vacancie
- B. The chief information officer (CIO) approves security policy change
- C. The information security oversight committee only meets quarterl
- D. The data center manager has final signoff on all security project

**Answer:** D

**Explanation:**

A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good, qualified information security professionals.

#### NEW QUESTION 81

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 86

Who should drive the risk analysis for an organization?

- A. Senior management

- B. Security manager
- C. Quality manager
- D. Legal department

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 87

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 91

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 93

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 94

Acceptable risk is achieved when:

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 95

After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

- A. Senior management
- B. Business manager
- C. IT audit manager
- D. Information security officer (ISO)

**Answer: B**

#### Explanation:

The business manager will be in the best position, based on the risk assessment and mitigation proposals. to decide which controls should/could be implemented, in line with the business strategy and with budget. Senior management will have to ensure that the business manager has a clear understanding of the risk assessed but in no case will be in a position to decide on specific controls. The IT audit manager will take part in the process to identify threats and vulnerabilities, and to make recommendations for mitigations. The information security officer (ISO) could make some decisions regarding implementation of controls. However, the business manager will have a broader business view and full control over the budget and, therefore, will be in a better position to make strategic decisions.

#### NEW QUESTION 97

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 101

Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

- A. Gap analysis
- B. Regression analysis
- C. Risk analysis
- D. Business impact analysis

**Answer: D**

#### Explanation:

Recovery time objectives (RTOs) are a primary deliverable of a business impact analysis. RTOs relate to the financial impact of a system not being available. A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules. Risk analysis is a component of the business impact analysis.

#### NEW QUESTION 104

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 108

All risk management activities are PRIMARILY designed to reduce impacts to:

- A. a level defined by the security manage
- B. an acceptable level based on organizational risk toleranc
- C. a minimum level consistent with regulatory requirement
- D. the minimum level possibl

**Answer: B**

**Explanation:**

The aim of risk management is to reduce impacts to an acceptable level. "Acceptable" or "reasonable" are relative terms that can vary based on environment and circumstances. A minimum level that is consistent with regulatory requirements may not be consistent with business objectives, and regulators typically do not assign risk levels. The minimum level possible may not be aligned with business requirements.

**NEW QUESTION 109**

Attackers who exploit cross-site scripting vulnerabilities take advantage of:

- A. a lack of proper input validation control
- B. weak authentication controls in the web application layer
- C. flawed cryptographic secure sockets layer (SSL) implementations and short key length
- D. implicit web application trust relationship

**Answer: A**

**Explanation:**

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSL) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

**NEW QUESTION 110**

The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

- A. periodically testing the incident response plan
- B. regularly testing the intrusion detection system (IDS).
- C. establishing mandatory training of all personnel
- D. periodically reviewing incident response procedure

**Answer: A**

**Explanation:**

Security incident response plans should be tested to find any deficiencies and improve existing processes. Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation. All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended. Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

**NEW QUESTION 111**

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 114**

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 115**

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

- A. Defining job roles
- B. Performing a risk assessment

- C. Identifying data owners
- D. Establishing data retention policies

**Answer:** C

**Explanation:**

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

**NEW QUESTION 119**

What does a network vulnerability assessment intend to identify?

- A. 0-day vulnerabilities
- B. Malicious software and spyware
- C. Security design flaws
- D. Misconfiguration and missing updates

**Answer:** D

**Explanation:**

A network vulnerability assessment intends to identify known vulnerabilities based on common misconfigurations and missing updates. 0-day vulnerabilities by definition are not previously known and therefore are undetectable. Malicious software and spyware are normally addressed through antivirus and antispyware policies. Security design flaws require a deeper level of analysis.

**NEW QUESTION 121**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 123**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 128**

Which of the following is the PRIMARY reason for implementing a risk management program?

- A. Allows the organization to eliminate risk
- B. Is a necessary part of management's due diligence
- C. Satisfies audit and regulatory requirements
- D. Assists in incrementing the return on investment (ROI)

**Answer:** B

**Explanation:**

The key reason for performing risk management is that it is part of management's due diligence. The elimination of all risk is not possible. Satisfying audit and regulatory requirements is of secondary importance. A risk management program may or may not increase the return on investment (ROI).

**NEW QUESTION 132**

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 replacement

**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 136

Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

- A. Business continuity coordinator
- B. Chief operations officer (COO)
- C. Information security manager
- D. Internal audit

**Answer:** B

**Explanation:**

The recovery point objective (RPO) is the processing checkpoint to which systems are recovered. In addition to data owners, the chief operations officer (COO) is the most knowledgeable person to make this decision. It would be inappropriate for the information security manager or an internal audit to determine the RPO because they are not directly responsible for the data or the operation.

#### NEW QUESTION 137

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 139

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 140

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 142

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) attac
- C. abuse a race conditio
- 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 145**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 149**

Which of the following are the essential ingredients of a business impact analysis (BIA)?

- A. Downtime tolerance, resources and criticality
- B. Cost of business outages in a year as a factor of the security budget
- C. Business continuity testing methodology being deployed
- D. Structure of the crisis management team

**Answer:** A

**Explanation:**

The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function. Options B, C and D are all associated with business continuity planning, but are not related to the BIA.

**NEW QUESTION 152**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 157**

A risk analysis should:

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 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 losses
- B. recommend not renewing the contract upon expiration
- C. recommend the immediate termination of the contract
- D. determine the current level of security

**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 outsourcing 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 166

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 168

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

- A. mitigate the impact by purchasing insurance
- B. implement a circuit-level firewall to protect the network
- C. increase the resiliency of security measures in place
- D. implement a real-time intrusion detection system

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 170

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 172

The valuation of IT assets should be performed by:

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

**Answer:** D

**Explanation:**

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter

expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

#### NEW QUESTION 173

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- A. Historical cost of the asset
- B. Acceptable level of potential business impacts
- C. Cost versus benefit of additional mitigating controls
- D. Annualized loss expectancy (ALE)

**Answer: C**

#### Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

#### NEW QUESTION 176

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 180

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 183

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 187

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 191**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 194**

The purpose of a corrective control is to:

- A. reduce adverse event
- B. indicate compromise
- C. mitigate impact
- D. ensure compliance

**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 199**

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 204**

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 209**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 210**

Who is responsible for ensuring that information is classified?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 211**

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 213**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 218**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 220**

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 221

When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

- A. Estimated productivity losses
- B. Possible scenarios with threats and impacts
- C. Value of information assets
- D. Vulnerability assessment

**Answer: B**

**Explanation:**

Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

#### NEW QUESTION 225

When residual risk is minimized:

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 228

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

- A. Customer data stolen
- B. An electrical power outage
- C. A web site defaced by hackers
- D. Loss of the software development team

**Answer: B**

**Explanation:**

The effect of the theft of customer data or web site defacement by hackers could lead to a permanent decline in customer confidence, which does not lend itself to measurement by quantitative techniques. Loss of a majority of the software development team could have similar unpredictable repercussions. However, the loss of electrical power for a short duration is more easily measurable and can be quantified into monetary amounts that can be assessed with quantitative techniques.

#### NEW QUESTION 233

Which of the following will BEST prevent external security attacks?

- A. Static IP addressing
- B. Network address translation
- C. Background checks for temporary employees
- D. Securing and analyzing system access logs

**Answer: B**

**Explanation:**

Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

#### NEW QUESTION 235

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 238

In assessing risk, it is MOST essential to:

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 240

An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

- A. eliminating the ris
- B. transferring the ris
- C. mitigating the ris
- D. accepting the ris

**Answer: C**

#### Explanation:

Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

#### NEW QUESTION 243

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 244

The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

- A. Mitigating controls
- B. Visibility of impact
- C. Likelihood of occurrence
- D. Incident frequency

**Answer: B**

#### Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not

as relevant. Mitigating controls is not a determining factor on incident reporting.

#### NEW QUESTION 249

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 252

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 254

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 258

When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

- A. The firewall should block all inbound traffic during the outage
- B. All systems should block new logins until the problem is corrected
- C. Access control should fall back to no synchronized mode
- D. System logs should record all user activity for later analysis

**Answer: C**

#### Explanation:

The best mechanism is for the system to fallback to the original process of logging on individually to each system. Blocking traffic and new logins would be overly restrictive to the conduct of business, while recording all user activity would add little value.

#### NEW QUESTION 261

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 266

A test plan to validate the security controls of a new system should be developed during which phase of the project?

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

**Answer: C**

#### Explanation:

In the design phase, security checkpoints are defined and a test plan is developed. The testing phase is too late since the system has already been developed and is in production testing. In the initiation phase, the basic security objective of the project is acknowledged. Development is the coding phase and is too late to consider test plans.

#### NEW QUESTION 267

An information security program should be sponsored by:

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 270

Who can BEST approve plans to implement an information security governance framework?

- A. Internal auditor
- B. Information security management
- C. Steering committee
- D. Infrastructure management

**Answer: C**

#### Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

#### NEW QUESTION 271

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 273

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 276

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

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

**Answer:** A

**Explanation:**

The authentication process is broken because, although the session is valid, the application should reauthenticate when the input parameters are changed. The review provided valid employee IDs, and valid input was processed. The problem here is the lack of reauthentication when the input parameters are changed. Cross-site scripting is not the problem in this case since the attack is not transferred to any other user's browser to obtain the output. Structured query language (SQL) injection is not a problem since input is provided as a valid employee ID and no SQL queries are injected to provide the output.

#### NEW QUESTION 278

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 283

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 288

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 289

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 292

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 294

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 297

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 298

Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

- A. Patch management
- B. Change management
- C. Security baselines
- D. Virus detection

**Answer:** B

**Explanation:**

Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses. Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

#### NEW QUESTION 300

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 301

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 302

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 305

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 309

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

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

**Answer:** D

**Explanation:**

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

management is a key component.

#### NEW QUESTION 312

Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

- A. Authentication
- B. Hardening
- C. Encryption
- D. Nonrepudiation

**Answer: C**

#### Explanation:

Cardholder data should be encrypted using strong encryption techniques. Hardening would be secondary in importance, while nonrepudiation would not be as relevant. Authentication of the point-of-sale (POS) terminal is a previous step to acquiring the card information.

#### NEW QUESTION 313

Nonrepudiation can BEST be ensured by using:

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 318

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 320

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

- A. customize the content to the target audienc
- B. ensure senior management is represente
- C. ensure that all the staff is traine
- 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 322

On which of the following should a firewall be placed?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 327

In an organization, information systems security is the responsibility of:

- A. all personne
- B. information systems personne
- C. information systems security personne
- D. functional personne

**Answer:** A

#### Explanation:

All personnel of the organization have the responsibility of ensuring information systems security-this can include indirect personnel such as physical security personnel. Information systems security cannot be the responsibility of information systems personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of information systems security personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of functional personnel alone since they cannot ensure security.

#### NEW QUESTION 332

When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

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

**Answer:** B

#### Explanation:

Comparison of cost of achievement of control objectives and corresponding value of assets sought to be protected would provide a sound basis for the information security manager to measure value delivery. Number of controls has no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated. Effectiveness of controls has no correlation with the value of assets unless their costs are also evaluated. Test results of controls have no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated.

#### NEW QUESTION 333

The information classification scheme should:

- A. consider possible impact of a security breac
- B. classify personal information in electronic for
- C. be performed by the information security manage
- D. classify systems according to the data processe

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 335

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 338

The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

- A. ensure the confidentiality of sensitive materia
- B. provide a high assurance of identit

- C. allow deployment of the active director
- D. implement secure sockets layer (SSL) encryptio

**Answer:** B

**Explanation:**

The primary purpose of a public key infrastructure (PKI) is to provide strong authentication. Confidentiality is a function of the session keys distributed by the PKI. An active directory can use PKI for authentication as well as using other means. Even though secure sockets layer (SSL) encryption requires keys to authenticate, it is not the main reason for deploying PKI.

#### NEW QUESTION 342

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 344

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 349

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- A. a strong authenticatio
- B. IP antispoofing filterin
- C. network encryption protoco
- D. access lists of trusted device

**Answer:** A

**Explanation:**

Strong authentication will provide adequate assurance on the identity of the users, while IP antispoofing is aimed at the device rather than the user. Encryption protocol ensures data confidentiality and authenticity while access lists of trusted devices are easily exploited by spoofed identity of the clients.

#### NEW QUESTION 354

Security awareness training is MOST likely to lead to which of the following?

- A. Decrease in intrusion incidents
- B. Increase in reported incidents
- C. Decrease in security policy changes
- D. Increase in access rule violations

**Answer:** B

**Explanation:**

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

#### NEW QUESTION 359

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 363

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 365

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 368

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

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

**Answer:** C

**Explanation:**

The IT manager needs to report the security risks in the environment pursuant to the security review, including risks in the IT implementation. Choices A, B and D are important, but not the main responsibilities or job requirements.

#### NEW QUESTION 371

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 372

Security awareness training should be provided to new employees:

- A. on an as-needed basi
- B. during system user trainin
- C. before they have access to dat
- D. along with department staf

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 377

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 378

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 380

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 381

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 385

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

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

**Answer: D**

**Explanation:**

Role-based access controls will grant temporary employee access based on the job function to be performed. This provides a better means of ensuring that the access is not more or less than what is required. Discretionary, mandatory and lattice-based access controls are all security models, but they do not address the issue of temporary employees as well as role-based access controls.

#### NEW QUESTION 390

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. polic
- B. strateg
- C. guideline
- D. baselin

**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 395

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 397

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 401

An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

- A. Right to audit
- B. Nondisclosure agreement
- C. Proper firewall implementation
- D. Dedicated security manager for monitoring compliance

**Answer: A**

**Explanation:**

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a

business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

#### NEW QUESTION 402

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 406

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

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

**Answer: C**

#### Explanation:

End users may react differently to the implementation, and may have specific preferences.

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

#### NEW QUESTION 409

Information security policies should:

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 412

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 417

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 422

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 427

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 430

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 434

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 438

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 443

An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

- A. validate and sanitize client side input
- B. harden the database listener componen
- C. normalize the database schema to the third normal for
- D. ensure that the security patches are updated on operating system

**Answer:** A

#### Explanation:

SQL injection vulnerability arises when crafted or malformed user inputs are substituted directly in SQL queries, resulting into information leakage. Hardening the database listener does enhance the security of the database; however, it is unrelated to the SQL injection vulnerability. Normalization is related to the effectiveness and efficiency of the database but not to SQL injection vulnerability. SQL injections may also be observed in normalized databases. SQL injection vulnerability exploits the SQL query design, not the operating system.

#### NEW QUESTION 445

.....

## 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](#)**