



**Isaca**

**Exam Questions CISM**

Certified Information Security Manager

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

When personal information is transmitted across networks, there MUST be adequate controls over:

- A. change management
- B. privacy protection
- C. consent to data transfer
- D. encryption device

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 2

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 3

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 4

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

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

**Answer: A**

#### Explanation:

The steering committee controls the execution of the information security strategy according to the needs of the organization and decides on the project prioritization and the execution plan. The steering committee does not allocate department budgets for business units. While ensuring that regulatory oversight requirements are met could be a consideration, it is not the main reason for the review. Reducing the impact on the business units is a secondary concern but not the main reason for the review.

#### NEW QUESTION 5

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

- A. Obtain the support of the board of 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 ( ' are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

**NEW QUESTION 6**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

Investments in information security technologies should be based on:

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 8**

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 9**

An organization's information security strategy should be based on:

- A. managing risk relative to business objective
- B. managing risk to a zero level and minimizing insurance premium
- C. avoiding occurrence of risks so that insurance is not required
- D. transferring most risks to insurers and saving on control cost

**Answer:** A

**Explanation:**

Organizations must manage risks to a level that is acceptable for their business model, goals and objectives. A zero-level approach may be costly and not provide the effective benefit of additional revenue to the organization. Long-term maintenance of this approach may not be cost effective. Risks vary as business models, geography, and regulatory- and operational processes change. Insurance covers only a small portion of risks and requires that the organization have certain operational controls in place.

**NEW QUESTION 10**

The PRIMARY objective of a security steering group is to:

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

**Answer: B**

**Explanation:**

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

#### NEW QUESTION 10

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

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 11

Information security policy enforcement is the responsibility of the:

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

**Answer: C**

**Explanation:**

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

#### NEW QUESTION 12

Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

- A. Alignment with industry best practices
- B. Business continuity investment
- C. Business benefits
- D. Regulatory compliance

**Answer: D**

**Explanation:**

Regulatory compliance can be a standalone driver for an information security governance measure. No further analysis nor justification is required since the entity has no choice in the regulatory requirements. Buy-in from business managers must be obtained by the information security manager when an information security governance measure is sought based on its alignment with industry best practices. Business continuity investment needs to be justified by business impact analysis. When an information security governance measure is sought based on qualitative business benefits, further analysis is required to determine whether the benefits outweigh the cost of the information security governance measure in question.

#### NEW QUESTION 17

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 20

Investment in security technology and processes should be based on:

- A. clear alignment with the goals and objectives of the organization
- B. success cases that have been experienced in previous project
- C. best business practice
- D. safeguards that are inherent in existing technology

**Answer:** A

#### Explanation:

Organization maturity level for the protection of information is a clear alignment with goals and objectives of the organization. Experience in previous projects is dependent upon other business models which may not be applicable to the current model. Best business practices may not be applicable to the organization's business needs. Safeguards inherent to existing technology are low cost but may not address all business needs and/or goals of the organization.

#### NEW QUESTION 22

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 27

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 32

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 37

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 38

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 39

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 42

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 47

Which of the following is the MOST important element of an information security strategy?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 50

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 53**

Minimum standards for securing the technical infrastructure should be defined in a security:

- A. strateg
- B. guideline
- C. mode
- D. architectur

**Answer: D**

**Explanation:**

Minimum standards for securing the technical infrastructure should be defined in a security architecture document. This document defines how components are secured and the security services that should be in place. A strategy is a broad, high-level document. A guideline is advisory in nature, while a security model shows the relationships between components.

**NEW QUESTION 54**

The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

- A. generally accepted industry best practice
- B. business requirement
- C. legislative and regulatory requirement
- D. storage availabilit

**Answer: B**

**Explanation:**

The primary concern will be to comply with legislation and regulation but only if this is a genuine business requirement. Best practices may be a useful guide but not a primary concern. Legislative and regulatory requirements are only relevant if compliance is a business need. Storage is irrelevant since whatever is needed must be provided

**NEW QUESTION 59**

Reviewing which of the following would BEST ensure that security controls are effective?

- A. Risk assessment policies
- B. Return on security investment
- C. Security metrics
- D. User access rights

**Answer: C**

**Explanation:**

Reviewing security metrics provides senior management a snapshot view and trends of an organization's security posture. Choice A is incorrect because reviewing risk assessment policies would not ensure that the controls are actually working. Choice B is incorrect because reviewing returns on security investments provides business justifications in implementing controls, but does not measure effectiveness of the control itself. Choice D is incorrect because reviewing user access rights is a joint responsibility of the data custodian and the data owner, and does not measure control effectiveness.

**NEW QUESTION 60**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 65**

The MOST important characteristic of good security policies is that they:

- A. state expectations of IT managemen
- B. state only one general security mandat
- C. are aligned with organizational goal
- D. govern the creation of procedures and guideline



**Answer:** C

**Explanation:**

The most important characteristic of good security policies is that they be aligned with organizational goals. Failure to align policies and goals significantly reduces the value provided by the policies. Stating expectations of IT management omits addressing overall organizational goals and objectives. Stating only one general security mandate is the next best option since policies should be clear; otherwise, policies may be confusing and difficult to understand. Governing the creation of procedures and guidelines is most relevant to information security standards.

#### NEW QUESTION 67

While implementing information security governance an organization should FIRST:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 68

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 71

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 72

Retention of business records should PRIMARILY be based on:

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 75

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 79

In implementing information security governance, the information security manager is PRIMARILY responsible for:

- A. developing the security strateg
- B. reviewing the security strateg
- C. communicating the security strateg
- D. approving the security strategy

**Answer:** A

**Explanation:**

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

#### NEW QUESTION 81

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 85

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 lif
- B. regulatory and legal requirement
- C. business strategy and directio
- D. application systems and medi

**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 90

Which of the following is the BEST justification to convince management to invest in an information security program?

- A. Cost reduction
- B. Compliance with company policies
- C. Protection of business assets
- D. Increased business value

**Answer:** D

**Explanation:**

Investing in an information security program should increase business value and confidence. Cost reduction by itself is rarely the motivator for implementing an information security program. Compliance is secondary to business value. Increasing business value may include protection of business assets.

#### NEW QUESTION 92

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

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

**Answer: B**

**Explanation:**

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

#### NEW QUESTION 96

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 97

Logging is an example of which type of defense against systems compromise?

- A. Containment
- B. Detection
- C. Reaction
- D. Recovery

**Answer: B**

**Explanation:**

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

#### NEW QUESTION 99

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

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

**Answer: B**

**Explanation:**

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

#### NEW QUESTION 100

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

- A. legal departmen
- B. compliance office
- C. information security manage
- D. business owne

**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 103

The MOST appropriate role for senior management in supporting information security is the:

- A. evaluation of vendors offering security product
- B. assessment of risks to the organizatio
- C. approval of policy statements and fundin
- D. monitoring adherence to regulatory requirement

**Answer: C**

#### Explanation:

Since the members of senior management are ultimately responsible for information security, they are the ultimate decision makers in terms of governance and direction. They are responsible for approval of major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager; in some organizations, business management is involved in these other activities, though their primary role is direction and governance.

#### NEW QUESTION 105

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 107

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 110

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 114

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 116

Which of the following characteristics is MOST important when looking at prospective candidates for the role of chief information security officer (CISO)?

- A. Knowledge of information technology platforms, networks and development methodologies
- B. Ability to understand and map organizational needs to security technologies
- C. Knowledge of the regulatory environment and project management techniques
- D. Ability to manage a diverse group of individuals and resources across an organization

**Answer: B**

#### Explanation:

Information security will be properly aligned with the goals of the business only with the ability to understand and map organizational needs to enable security technologies. All of the other choices are important but secondary to meeting business security needs.

#### NEW QUESTION 121

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 124

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 126

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 131

Relationships among security technologies are BEST defined through which of the following?

- A. Security metrics
- B. Network topology
- C. Security architecture
- D. Process improvement models



**Answer:** C

**Explanation:**

Security architecture explains the use and relationships of security mechanisms. Security metrics measure improvement within the security practice but do not explain the use and relationships of security technologies. Process improvement models and network topology diagrams also do not describe the use and relationships of these technologies.

#### NEW QUESTION 135

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

- A. return on investment (ROI)
- B. a vulnerability assessment
- C. annual loss expectancy (ALE).
- D. a business case

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 136

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 139

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 140

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 142

Which of the following authentication methods prevents authentication replay?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 143

Acceptable risk is achieved when:

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 146

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 151

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 154

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 159**

Risk management programs are designed to reduce risk to:

- A. a level that is too small to be measurable
- B. the point at which the benefit exceeds the expense
- C. a level that the organization is willing to accept
- D. a rate of return that equals the current cost of capital

**Answer: C**

**Explanation:**

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

**NEW QUESTION 164**

An organization has to comply with recently published industry regulatory requirements—compliance that potentially has high implementation costs. What should the information security manager do FIRST?

- A. Implement a security committee
- B. Perform a gap analysis
- C. Implement compensating controls
- D. Demand immediate compliance

**Answer: B**

**Explanation:**

Since they are regulatory requirements, a gap analysis would be the first step to determine the level of compliance already in place. Implementing a security committee or compensating controls would not be the first step. Demanding immediate compliance would not assess the situation.

**NEW QUESTION 167**

The BEST strategy for risk management is to:

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 169**

When performing an information risk analysis, an information security manager should FIRST:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 170**

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 175

Risk acceptance is a component of which of the following?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 177

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 178

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 antispayware policies. Security design flaws require a deeper level of analysis.

#### NEW QUESTION 182

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

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

**Answer:** A

**Explanation:**

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

#### NEW QUESTION 185

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 189

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 191

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 (ROD)

**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 (ROD).

#### NEW QUESTION 192

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 196

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 201

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 205**

A risk mitigation report would include recommendations for:

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 208**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 211**

Risk assessment is MOST effective when performed:

- A. at the beginning of security program developmen
- B. on a continuous basi
- C. while developing the business case for the security progra
- D. during the business change proces

**Answer: B**

**Explanation:**

Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

**NEW QUESTION 213**

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 218**

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

- A. gain control through a buffer overflo
- 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 221**

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 225**

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 227**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 228**

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

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

**Answer: D**

**Explanation:**

Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

**NEW QUESTION 230**

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

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

**Answer: C**



**Explanation:**

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

**NEW QUESTION 233**

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 outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

**NEW QUESTION 238**

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 240**

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 243**

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 245**

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

- A. organizational requirement
- B. information systems requirement
- C. information security requirement

D. international standard

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 246

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 251

A risk management program should reduce risk to:

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 255

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 257

Which of the following will BEST protect an organization from internal security attacks?

- A. Static IP addressing
- B. Internal address translation
- C. Prospective employee background checks
- D. Employee awareness certification program

**Answer:** C

**Explanation:**

Because past performance is a strong predictor of future performance, background checks of prospective employees best prevents attacks from originating within an organization. Static IP addressing does little to prevent an internal attack. Internal address translation using non-routable addresses is useful against external attacks but not against internal attacks. Employees who certify that they have read security policies are desirable, but this does not guarantee that the employees behave honestly.

#### NEW QUESTION 261

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 262

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 264

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 265

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 266

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 269

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- A. Prevent the system from being accessed remotely
- B. Create a strong random password
- C. Ask for a vendor patch
- D. Track usage of the account by audit trails

**Answer: B**

#### Explanation:

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

#### NEW QUESTION 273

The purpose of a corrective control is to:

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 275

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 279

In a business impact analysis, the value of an information system should be based on the overall cost:

- A. of recover
- B. to recreat
- C. if unavailabl
- D. of emergency operation

**Answer: C**

#### Explanation:

The value of an information system should be based on the cost incurred if the system were to become unavailable. The cost to design or recreate the system is not as relevant since a business impact analysis measures the impact that would occur if an information system were to become unavailable. Similarly, the cost of emergency operations is not as relevant.

#### NEW QUESTION 283

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

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

**Answer: C**

#### Explanation:

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

confidentiality of information.

#### NEW QUESTION 287

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 289

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 293

For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

- A. Biometrics
- B. Symmetric encryption keys
- C. Secure Sockets Layer (SSL)-based authentication
- D. Two-factor authentication

**Answer: D**

#### Explanation:

Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

#### NEW QUESTION 295

When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

- A. IP spoofing
- B. Man-in-the-middle attack
- C. Repudiation
- D. Trojan

**Answer: D**

#### Explanation:

A Trojan is a program that gives the attacker full control over the infected computer, thus allowing the attacker to hijack, copy or alter information after authentication by the user. IP spoofing will not work because IP is not used as an authentication mechanism. Man-in-the-middle attacks are not possible if using SSL with client-side certificates. Repudiation is unlikely because client-side certificates authenticate the user.

#### NEW QUESTION 296

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 300

The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

- A. Secure Sockets Layer (SSL).
- B. Secure Shell (SSH).
- C. IP Security (IPSec).
- D. Secure/Multipurpose Internet Mail Extensions (S/MIME ).

**Answer:** A

**Explanation:**

Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet. In typical use, all data transmitted between the customer and the business are, therefore, encrypted by the business's web server and remain confidential. SSH File Transfer Protocol (SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with the SSH-2 protocol to provide secure file transfer. IP Security (IPSec) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPSec operation: transport mode and tunnel mode. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of e-mail encapsulated in MIME; it is not a web transaction protocol.

#### NEW QUESTION 305

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 309

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 312

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 315



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 317

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- A. Security in storage and transmission of sensitive data
- B. Provider's level of compliance with industry standards
- C. Security technologies in place at the facility
- D. Results of the latest independent security review

**Answer: A**

**Explanation:**

Now the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

#### NEW QUESTION 322

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

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 323

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

- A. develop a risk assessment plan
- B. develop a data protection plan
- C. protect information assets and resources
- D. establish security governance

**Answer: C**

**Explanation:**

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

#### NEW QUESTION 327

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 330

Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

- A. Tuning
- B. Patching
- C. Encryption
- D. Packet filtering

**Answer: A**

#### Explanation:

If an intrusion detection system (IDS) is not properly tuned it will generate an unacceptable number of false positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to operating system hardening, while encryption and packet filtering would not be as relevant.

#### NEW QUESTION 333

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 338

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 342

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 347

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 352**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 357**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 359**

Which of the following devices should be placed within a DMZ?

- A. Router
- B. Firewall
- C. Mail relay
- D. Authentication server

**Answer: C**

**Explanation:**

A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ, network segment.

**NEW QUESTION 363**

Which of the following would be the BEST defense against sniffing?

- A. Password protect the files
- B. Implement a dynamic IP address scheme
- C. Encrypt the data being transmitted
- D. Set static mandatory access control (MAC) addresses

**Answer: C**

**Explanation:**

Encrypting the data will obfuscate the data so that they are not visible in plain text. Someone would have to collate the entire data stream and try decrypting it, which is not easy. Passwords can be recovered by brute-force attacks and by password crackers, so this is not the best defense against sniffing. IP addresses can always be discovered, even if dynamic IP addresses are implemented. The person sniffing traffic can initiate multiple sessions for possible IP addresses. Setting static mandatory access control (MAC) addresses can prevent address resolution protocol (ARP) poisoning, but it does not prevent sniffing.

**NEW QUESTION 367**

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 372

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 374

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 378

Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 383

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 388

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 392

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 395

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

- A. ensure the confidentiality of sensitive material
- B. provide a high assurance of identity
- C. allow deployment of the active directory
- D. implement secure sockets layer (SSL) encryption

**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 400

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 403

The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

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

**Answer:** A

**Explanation:**

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



#### NEW QUESTION 407

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 409

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

- A. the parties to the agreement can perform
- B. confidential data are not included in the agreement
- C. appropriate controls are included
- D. the right to audit is a requirement

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 414

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 418

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 419

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

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

**Answer: D**



**Explanation:**

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

**NEW QUESTION 422**

When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

- A. access control matrix
- B. encryption strength
- C. authentication mechanism
- D. data repository

**Answer:** A

**Explanation:**

The access control matrix is the best indicator of the level of compliance with the service level agreement (SLA) data confidentiality clauses. Encryption strength, authentication mechanism and data repository might be defined in the SLA but are not confidentiality compliance indicators.

**NEW QUESTION 427**

A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 430**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 431**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 432**

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 433

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 437

Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

- A. define the circumstances where cryptography should be use
- B. define cryptographic algorithms and key length
- C. describe handling procedures of cryptographic key
- D. establish the use of cryptographic solution

**Answer:** A

**Explanation:**

There should be documented standards- procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

#### NEW QUESTION 442

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 446

To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

- A. Service level agreements (SLAs)
- B. Right to audit clause
- C. Intrusion detection system (IDS) services
- D. Spam filtering services

**Answer:** A

**Explanation:**

Service level agreements (QUESTION NO: As) will be most effective in ensuring that Internet service providers (ISPs) comply with expectations for service availability. Intrusion detection system (IDS) and spam filtering services would not mitigate (as directly) the potential for service interruptions. A right-to-audit clause would not be effective in mitigating the likelihood of a service interruption.

#### NEW QUESTION 451

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 456

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 460

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 465

Security audit reviews should PRIMARILY:

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 466

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 470

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 474

The PRIMARY focus of the change control process is to ensure that changes are:

- A. authorize
- B. applie
- C. documente
- D. teste

**Answer:** A

#### Explanation:

All steps in the change control process must be signed off on to ensure proper authorization. It is important that changes are applied, documented and tested; however, they are not the primary focus.

#### NEW QUESTION 479

Security policies should be aligned MOST closely with:

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 483

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 486

.....

## Relate Links

**100% Pass Your CISM Exam with ExamBible Prep Materials**

<https://www.exambible.com/CISM-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>