

CISM Dumps

Certified Information Security Manager

<https://www.certleader.com/CISM-dumps.html>



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 is responsible for legal and regulatory liability?

- A. Chief security officer (CSO)
- B. Chief legal counsel (CLC)
- C. Board and senior management
- D. Information security steering group

Answer: C

Explanation:

The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: D

Explanation:

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

NEW QUESTION 5

A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the information security program?

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

Answer: C

Explanation:

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

NEW QUESTION 6

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

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

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

Answer: C

Explanation:

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

NEW QUESTION 8

Which of the following MOST commonly falls within the scope of an information security governance steering committee?

- A. Interviewing candidates for information security specialist positions
- B. Developing content for security awareness programs
- C. Prioritizing information security initiatives
- D. Approving access to critical financial systems

Answer: C

Explanation:

Prioritizing information security initiatives is the only appropriate item. The interviewing of specialists should be performed by the information security manager, while the developing of program content should be performed by the information security staff. Approving access to critical financial systems is the responsibility of individual system data owners.

NEW QUESTION 9

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 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

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

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

Answer: B

Explanation:

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

NEW QUESTION 14

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 22

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 26

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

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

Answer: A

Explanation:

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

NEW QUESTION 30

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

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

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 35

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 40

From an information security perspective, information that no longer supports the main purpose of the business should be:

- A. analyzed under the retention policy
- B. protected under the information classification policy
- C. analyzed under the backup policy
- D. protected under the business impact analysis (BIA).

Answer: A

Explanation:

Option A is the type of analysis that will determine whether the organization is required to maintain the data for business, legal or regulatory reasons. Keeping data that are no longer required unnecessarily consumes resources, and, in the case of sensitive personal information, can increase the risk of data compromise. Options B, C and D are attributes that should be considered in the destruction and retention policy. A BIA could help determine that this information does not support the main objective of the business, but does not indicate the action to take.

NEW QUESTION 41

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BEST approach of the information security manager?

- A. Acceptance of the business manager's decision on the risk to the corporation
- B. Acceptance of the information security manager's decision on the risk to the corporation
- C. Review of the assessment with executive management for final input
- D. A new risk assessment and BIA are needed to resolve the disagreement

Answer: C

Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large

financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

NEW QUESTION 42

Effective IT governance is BEST ensured by:

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

Answer: D

Explanation:

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

NEW QUESTION 44

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

- A. strategy
- B. guideline
- C. model
- D. architecture

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 48

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 52

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

- A. state expectations of IT management
- B. state only one general security mandate
- C. are aligned with organizational goals
- D. govern the creation of procedures and guidelines

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 57

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

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

Answer: A

Explanation:

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

NEW QUESTION 59

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 60

Who is ultimately responsible for the organization's information?

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

Answer: C

Explanation:

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

NEW QUESTION 64

A good privacy statement should include:

- A. notification of liability on accuracy of informatio
- B. notification that information will be encrypte
- C. what the company will do with information it collect
- D. a description of the information classification proces

Answer: C

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. Choice A is incorrect because that information should be located in the web site's disclaimer. Choice B is incorrect because, although encryption may be applied, this is not generally disclosed. Choice D is incorrect because information classification would be contained in a separate policy.

NEW QUESTION 68

Which of the following are seldom changed in response to technological changes?

- A. Standards
- B. Procedures
- C. Policies
- D. Guidelines

Answer: C

Explanation:

Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

NEW QUESTION 73

When implementing effective security governance within the requirements of the company's security strategy, which of the following is the MOST important factor to consider?

- A. Preserving the confidentiality of sensitive data
- B. Establishing international security standards for data sharing
- C. Adhering to corporate privacy standards
- D. Establishing system manager responsibility for information security

Answer: A

Explanation:

The goal of information security is to protect the organization's information assets. International security standards are situational, depending upon the company and its business. Adhering to corporate privacy standards is important, but those standards must be appropriate and adequate and are not the most important factor to consider. All employees are responsible for information security, but it is not the most important factor to consider.

NEW QUESTION 76

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 79

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

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

Answer: A

Explanation:

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

NEW QUESTION 80

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 85

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 88

Which of the following represents the MAJOR focus of privacy regulations?

- A. Unrestricted data mining
- B. Identity theft
- C. Human rights protection
- D. Identifiable personal data

Answer: D

Explanation:

Protection of identifiable personal data is the major focus of recent privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Data mining is an accepted tool for ad hoc reporting; it could pose a threat to privacy only if it violates regulator)' provisions. Identity theft is a potential consequence of privacy violations but not the main focus of many regulations. Human rights addresses privacy issues but is not the main focus of regulations.

NEW QUESTION 92

Information security should be:

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

Answer: B

Explanation:

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

NEW QUESTION 97

Which of the following requirements would have the lowest level of priority in information security?

- A. Technical
- B. Regulatory
- C. Privacy
- D. Business

Answer: A

Explanation:

Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

NEW QUESTION 102

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 107

A security manager meeting the requirements for the international flow of personal data will need to ensure:

- A. a data processing agreemen
- B. a data protection registratio
- C. the agreement of the data subject
- D. subject access procedure

Answer:

C

Explanation:

Whenever personal data are transferred across national boundaries, the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

NEW QUESTION 112

Who in an organization has the responsibility for classifying information?

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

Answer: D

Explanation:

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

NEW QUESTION 114

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 116

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 121

Who should drive the risk analysis for an organization?

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

Answer: B

Explanation:

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

NEW QUESTION 122

Information security projects should be prioritized on the basis of:

- A. time required for implementatio
- B. impact on the organizatio
- C. total cost for implementatio
- D. mix of resources require

Answer: B

Explanation:

Explanation:

Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

NEW QUESTION 124

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

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

Answer: C

Explanation:

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

NEW QUESTION 127

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

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

Answer: C

Explanation:

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

NEW QUESTION 131

The FIRST step to create an internal culture that focuses on information security is to:

- A. implement stronger controls
- B. conduct periodic awareness training
- C. actively monitor operations
- D. gain the endorsement of executive management

Answer: D

Explanation:

Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

NEW QUESTION 132

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 134

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 137

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

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

Answer: D

Explanation:

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

NEW QUESTION 142

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 information
- C. identify the value of the critical asset
- D. determine the financial impact if threats materialize

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 143

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 control
- 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 144

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

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

Answer: C

Explanation:

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

NEW QUESTION 146

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

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

Answer: C

Explanation:

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

NEW QUESTION 147

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

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

Answer: A

Explanation:

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

NEW QUESTION 148

Previously accepted risk should be:

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

Answer: A

Explanation:

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

NEW QUESTION 149

Phishing is BEST mitigated by which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 151

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

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

Answer: D

Explanation:

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

NEW QUESTION 153

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

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

Answer: B

Explanation:

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

NEW QUESTION 158

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

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

Answer: A

Explanation:

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

NEW QUESTION 161

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 165

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

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

Answer: D

Explanation:

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

NEW QUESTION 166

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 167

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 170

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 171

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

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

Answer: C

Explanation:

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

NEW QUESTION 173

A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

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

Answer: C

Explanation:

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

NEW QUESTION 176

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

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

Answer: C

Explanation:

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

NEW QUESTION 177

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 180

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

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

Answer: D

Explanation:

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

NEW QUESTION 183

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. transferred
- B. treated
- C. accepted
- D. terminated

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 184

A risk analysis should:

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

Answer: C

Explanation:

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

NEW QUESTION 188

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 193

Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

- A. Systems operation procedures are not enforced
- B. Change management procedures are poor
- C. Systems development is outsourced
- D. Systems capacity management is not performed

Answer: B

Explanation:

The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed by third-party vendors are becoming commonplace and do not represent an increase in security risk as much as poor change management. Poor capacity management may not necessarily represent a security risk.

NEW QUESTION 195

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

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

Answer: D

Explanation:

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

NEW QUESTION 200

The valuation of IT assets should be performed by:

- A. an IT security manage
- B. an independent security consultan
- C. the chief financial officer (CFO).
- D. the information owne

Answer: D

Explanation:

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

NEW QUESTION 202

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 207

A security risk assessment exercise should be repeated at regular intervals because:

- A. business threats are constantly changin
- B. omissions in earlier assessments can be addresse
- C. repetitive assessments allow various methodologie
- D. they help raise awareness on security in the busines

Answer: A

Explanation:

As business objectives and methods change, the nature and relevance of threats change as well. Choice B does not, by itself, justify regular reassessment. Choice C is not necessarily true in all cases. Choice D is incorrect because there are better ways of raising security awareness than by performing a risk assessment.

NEW QUESTION 209

For risk management purposes, the value of an asset should be based on:

- A. original cos
- B. net cash flo
- C. net present valu
- D. replacement cos

Answer: D

Explanation:

The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

NEW QUESTION 211

A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

- A. there are sufficient safeguards in place to prevent this risk from happenin
- B. the needed countermeasure is too complicated to deplo
- C. the cost of countermeasure outweighs the value of the asset and potential los
- D. The likelihood of the risk occurring is unknow

Answer: C

Explanation:

An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

NEW QUESTION 212

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 214

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 216

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 221

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 223

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

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

Answer: B

Explanation:

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

NEW QUESTION 228

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

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

Answer: B

Explanation:

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

NEW QUESTION 232

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

- A. total cost of ownership
- B. priority of restoration
- C. annualized loss expectancy (ALE).
- D. residual risk

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 235

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 239

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

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

Answer: B

Explanation:

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

NEW QUESTION 242

A risk management approach to information protection is:

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

Answer: A

Explanation:

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

NEW QUESTION 243

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

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

Answer: B

Explanation:

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

NEW QUESTION 245

An information security organization should PRIMARILY:

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

Answer:

A

Explanation:

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

NEW QUESTION 249

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 250

When performing a risk assessment, the MOST important consideration is that:

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

Answer: C

Explanation:

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

NEW QUESTION 254

Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

- A. Programming
- B. Specification
- C. User testing
- D. Feasibility

Answer: D

Explanation:

Risk should be addressed as early as possible in the development cycle. The feasibility study should include risk assessment so that the cost of controls can be estimated before the project proceeds. Risk should also be considered in the specification phase where the controls are designed, but this would still be based on the assessment carried out in the feasibility study. Assessment would not be relevant in choice A or C.

NEW QUESTION 257

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

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

Answer: B

Explanation:

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

NEW QUESTION 261

Which of the following will BEST prevent external security attacks?

- A. Static IP addressing
- B. Network address translation

- C. Background checks for temporary employees
- D. Securing and analyzing system access logs

Answer: B

Explanation:

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

NEW QUESTION 266

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

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

Answer: B

Explanation:

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

NEW QUESTION 270

Which of the following would be the FIRST step in establishing an information security program?

- A. Develop the security polic
- B. Develop security operating procedure
- C. Develop the security pla
- D. Conduct a security controls stud

Answer: C

Explanation:

A security plan must be developed to implement the security strategy. All of the other choices should follow the development of the security plan.

NEW QUESTION 273

An information security manager uses security metrics to measure the:

- A. performance of the information security progra
- B. performance of the security baselin
- C. effectiveness of the security risk analysi
- D. effectiveness of the incident response tea

Answer: A

Explanation:

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

NEW QUESTION 274

The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

- A. provide in-depth defens
- B. separate test and productio
- C. permit traffic load balancin
- D. prevent a denial-of-service attac

Answer: C

Explanation:

Having two entry points, each guarded by a separate firewall, is desirable to permit traffic load balancing. As they both connect to the Internet and to the same demilitarized zone (DMZ), such an arrangement is not practical for separating test from production or preventing a denial-of-service attack.

NEW QUESTION 278

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

- A. Server patching may be prevented
- B. System backups may be incomplete

- C. System integrity may be affected
- D. End-user sessions may be hijacked

Answer: C

Explanation:

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

NEW QUESTION 279

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 283

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

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

Answer: C

Explanation:

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

NEW QUESTION 284

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

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

Answer: A

Explanation:

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

NEW QUESTION 287

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

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

Answer: B

Explanation:

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

deviate traffic.

NEW QUESTION 288

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

- A. develop a risk assessment pla
- B. develop a data protection pla
- C. protect information assets and resource
- D. establish security governanc

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 H 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 289

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

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

Answer: C

Explanation:

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

NEW QUESTION 291

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

- A. Biometric authentication
- B. Embedded steganographic
- C. Two-factor authentication
- D. Embedded digital signature

Answer: D

Explanation:

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

NEW QUESTION 295

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

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

Answer: C

Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

NEW QUESTION 299

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

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

Answer: B

Explanation:

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

NEW QUESTION 300

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

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

Answer: A

Explanation:

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

NEW QUESTION 305

Security monitoring mechanisms should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 307

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 309

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

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

Answer: D

Explanation:

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

NEW QUESTION 314

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

- A. Configuration of firewalls
- B. Strength of encryption algorithms
- C. Authentication within application

D. Safeguards over keys

Answer: D

Explanation:

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

NEW QUESTION 316

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

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

Answer: B

Explanation:

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

NEW QUESTION 320

An e-commerce order fulfillment web server should generally be placed on which of the following?

- A. Internal network
- B. Demilitarized zone (DMZ)
- C. Database server
- D. Domain controller

Answer: B

Explanation:

An e-commerce order fulfillment web server should be placed within a DMZ to protect it and the internal network from external attack. Placing it on the internal network would expose the internal network to potential attack from the Internet. Since a database server should reside on the internal network, the same exposure would exist. Domain controllers would not normally share the same physical device as a web server.

NEW QUESTION 323

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

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

Answer: A

Explanation:

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

NEW QUESTION 327

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 331

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 333

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

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

Answer: A

Explanation:

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

NEW QUESTION 338

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

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

Answer: A

Explanation:

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

NEW QUESTION 342

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 344

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

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

Answer: D

Explanation:

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

NEW QUESTION 346

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 349

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 351

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

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

Answer: C

Explanation:

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

NEW QUESTION 353

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

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

Answer: A

Explanation:

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

NEW QUESTION 355

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

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

Answer: A

Explanation:

People are the weakest link in security implementation, and awareness would reduce this risk. Through security awareness and training programs, individual employees can be informed and sensitized on various security policies and other security topics, thus ensuring compliance from each individual. Laws and

regulations also aim to reduce human risk. Informing business units about the security strategy is best done through steering committee meetings or other forums.

NEW QUESTION 358

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 359

The information classification scheme should:

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

Answer: A

Explanation:

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

NEW QUESTION 360

An intrusion detection system should be placed:

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

Answer: C

Explanation:

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

NEW QUESTION 364

Which of the following is MOST effective in protecting against the attack technique known as phishing?

- A. Firewall blocking rules
- B. Up-to-date signature files
- C. Security awareness training
- D. Intrusion detection monitoring

Answer: C

Explanation:

Phishing relies on social engineering techniques. Providing good security awareness training will best reduce the likelihood of such an attack being successful. Firewall rules, signature files and intrusion detection system (IDS) monitoring will be largely unsuccessful at blocking this kind of attack.

NEW QUESTION 369

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 374

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

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

Answer: C

Explanation:

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

NEW QUESTION 375

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

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

Answer: B

Explanation:

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

NEW QUESTION 376

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

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

Answer: C

Explanation:

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

NEW QUESTION 380

Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

- A. An intrusion prevention system (IPS)
- B. An intrusion detection system (IDS)
- C. A host-based intrusion detection system (HIDS)
- D. A host-based firewall

Answer: A

Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect, but not prevent I IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

NEW QUESTION 383

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 387

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

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

Answer: D

Explanation:

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

NEW QUESTION 389

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

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

Answer: D

Explanation:

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

NEW QUESTION 391

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

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

Answer: D

Explanation:

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

NEW QUESTION 394

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 399

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 small
- 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 401

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

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

Answer: D

Explanation:

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

NEW QUESTION 406

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 411

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

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

Answer: B

Explanation:

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

NEW QUESTION 413

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

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

Answer: A

Explanation:

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

NEW QUESTION 416

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 420

Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

- A. the third party provides a demonstration on a test syste
- B. goals and objectives are clearly define
- C. the technical staff has been briefed on what to expec
- D. special backups of production servers are take

Answer: B

Explanation:

The most important action is to clearly define the goals and objectives of the test. Assuming that adequate backup procedures are in place, special backups should not be necessary. Technical staff should not be briefed nor should there be a demo as this will reduce the spontaneity of the test.

NEW QUESTION 425

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

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

Answer: A

Explanation:

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

NEW QUESTION 428

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

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

Answer: C

Explanation:

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

NEW QUESTION 431

Security audit reviews should PRIMARILY:

- A. ensure that controls operate as require
- B. ensure that controls are cost-effectiv
- C. focus on preventive control
- D. ensure controls are technologically curren

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 436

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

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

Answer: B

Explanation:

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

NEW QUESTION 440

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

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

Answer: C

Explanation:

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

NEW QUESTION 443

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

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

Answer: C

Explanation:

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

NEW QUESTION 445

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

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

Answer: D

Explanation:

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

NEW QUESTION 449

Which of the following is the MOST likely outcome of a well-designed information security awareness course?

- A. Increased reporting of security incidents to the incident response function
- B. Decreased reporting of security incidents to the incident response function
- C. Decrease in the number of password resets
- D. Increase in the number of identified system vulnerabilities

Answer: A

Explanation:

A well-organized information security awareness course informs all employees of existing security policies, the importance of following safe practices for data security and the need to report any possible security incidents to the appropriate individuals in the organization. The other choices would not be the likely outcomes.

NEW QUESTION 451

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

- A. Delivery path tracing
- B. Reverse lookup translation
- C. Out-of-band channels
- D. Digital signatures

Answer: C

Explanation:

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

NEW QUESTION 455

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISM Exam with Our Prep Materials Via below:

<https://www.certleader.com/CISM-dumps.html>