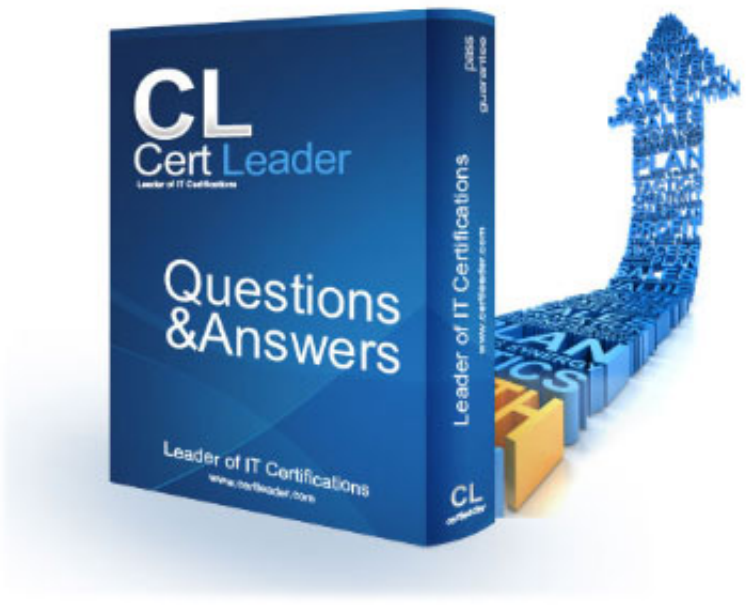
CISM Dumps

Certified Information Security Manager

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



NEW QUESTION 1
The FIRST step in establishing a security governance program is to:

A. conduct a risk assessmen
B. conduct a workshop for all end user
C. prepare a security budge
D. obtain high-level sponsorshi

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 2
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 3
Which of the following would BEST ensure the success of information security governance within an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 4
An outcome of effective security governance is:

A. business dependency assessment
B. strategic alignmen
C. risk assessmen
D. plannin

Answer: B

Explanation:

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

NEW QUESTION 5
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

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

Answer: D

Explanation:

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 7
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
Which of the following is the MOST important factor when designing information security architecture?

A. Technical platform interfaces
B. Scalability of the network
C. Development methodologies
D. Stakeholder requirements

Answer: D

Explanation:

The most important factor for information security is that it advances the interests of the business, as defined by stakeholder requirements. Interoperability and scalability, as well as development methodologies, are all important but are without merit if a technologically-elegant solution is achieved that does not meet the needs of the business.

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 10
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 15
Which of the following is a benefit of information security governance?

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

Answer: A

Explanation:

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

NEW QUESTION 17
Security technologies should be selected PRIMARILY on the basis of their:

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

Answer: A

Explanation:

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

NEW QUESTION 20
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

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

Answer: B

Explanation:

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

NEW QUESTION 25

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

A. analyzed under the retention polic
B. protected under the information classification polic
C. analyzed under the backup polic
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 30
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 BES T 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 34
Senior management commitment and support for information security can BEST be obtained through presentations that:

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

Answer: D

Explanation:

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

NEW QUESTION 37
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 40
Which of the following would BEST prepare an information security manager for regulatory reviews?

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

Answer: B

Explanation:

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

NEW QUESTION 42
The MOST important characteristic of good security policies is that they:

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

Answer: C

Explanation:

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

NEW QUESTION 44
In order to highlight to management the importance of network security, the security manager should FIRST:

A. develop a security architectur
B. install a network intrusion detection system (NIDS) and prepare a list of attack
C. develop a network security polic
D. conduct a risk assessmen

Answer: D

Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

NEW QUESTION 47
Retention of business records should PRIMARILY be based on:

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

Answer: B

Explanation:

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

NEW QUESTION 50
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

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

Answer: D

Explanation:

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

NEW QUESTION 51
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 55
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 60
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 63
What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

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

Answer: D

Explanation:

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

NEW QUESTION 66
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 69
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

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

Answer: B

Explanation:

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

NEW QUESTION 72
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 75
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 80
The data access requirements for an application should be determined by the:

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

Answer: D

Explanation:

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

NEW QUESTION 82
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

A. it implies compliance risk
B. short-term impact cannot be determine
C. it violates industry security practice
D. changes in the roles matrix cannot be detecte

Answer: A

Explanation:

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

NEW QUESTION 85
When developing an information security program, what is the MOST useful source of information for determining available resources?

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

Answer: D

Explanation:

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

NEW QUESTION 86
Which of the following roles would represent a conflict of interest for an information security manager?

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

Answer: C

Explanation:

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

NEW QUESTION 89
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 91
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 93
Senior management commitment and support for information security can BEST be enhanced through:

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

Answer: C

Explanation:

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

NEW QUESTION 96
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 100
Relationships among security technologies are BEST defined through which of the following?

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

Answer: C

Explanation:

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

NEW QUESTION 101
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: BExplanation:

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 102
An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

A. ensure that security processes are consistent across the organizatio
B. enforce baseline security levels across the organizatio
C. ensure that security processes are fully documente
D. implement monitoring of key performance indicators for security processe

Answer: A

Explanation:

The organization first needs to move from ad hoc to repeatable processes. The organization then needs to document the processes and implement process monitoring and measurement. Baselining security levels will not necessarily assist in process improvement since baselining focuses primarily on control improvement. The organization needs to standardize processes both before documentation, and before monitoring and measurement.

NEW QUESTION 106
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdiction
B. establish baseline standards for all locations and add supplemental standards as require
C. bring all locations into conformity with a generally accepted set of industry best practice
D. establish a baseline standard incorporating those requirements that all jurisdictions have in commo

Answer: B

Explanation:

It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach—forcing all locations to be in compliance with the regulations places an undue burden on those locations.

NEW QUESTION 110
Acceptable risk is achieved when:

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

Answer: A

Explanation:

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

NEW QUESTION 115
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 117
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 119
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

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

Answer: A

Explanation:

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

NEW QUESTION 123
One way to determine control effectiveness is by determining:

A. whether it is preventive, detective or compensator
B. the capability of providing notification of failur
C. the test results of intended objective
D. the evaluation and analysis of reliabilit

Answer: C

Explanation:

Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

NEW QUESTION 125
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 committe
B. Perform a gap analysi
C. Implement compensating control
D. Demand immediate complianc

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 126
The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

A. hourly billing rate charged by the carrie
B. value of the data transmitted over the networ
C. aggregate compensation of all affected business user
D. financial losses incurred by affected business unit

Answer: D

Explanation:

The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

NEW QUESTION 129
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

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

Answer: C

Explanation:

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

NEW QUESTION 133
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 137
What does a network vulnerability assessment intend to identify?

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

Answer: D

Explanation:

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

NEW QUESTION 138
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

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

Answer: B

Explanation:

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

NEW QUESTION 141
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 142
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 147
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 152
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

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

Answer: B

Explanation:

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

NEW QUESTION 157
The MAIN reason why asset classification is important to a successful information security program is because classification determines:

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

Answer: C

Explanation:

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

NEW QUESTION 162
Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

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

Answer: B

Explanation:

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

NEW QUESTION 167
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precis
B. security risks are subject to frequent chang
C. reviewers can optimize and reduce the cost of control
D. it demonstrates to senior management that the security function can add valu

Answer: B

Explanation:

Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

NEW QUESTION 169
After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

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

Answer: C

Explanation:

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

NEW QUESTION 174
A risk analysis should:

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

Answer: C

Explanation:

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

NEW QUESTION 176
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

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

Answer: A

Explanation:

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

NEW QUESTION 177
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 ris
C. Transfer the ris
D. Accept the ris

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 182
Which of the following attacks is BEST mitigated by utilizing strong passwords?

A. Man-in-the-middle attack
B. Brute force attack
C. Remote buffer overflow
D. Root kit

Answer: B

Explanation:

A brute force attack is normally successful against weak passwords, whereas strong passwords would not prevent any of the other attacks. Man-in-the-middle attacks intercept network traffic, which could contain passwords, but is not naturally password-protected. Remote buffer overflows rarely require a password to exploit a remote host. Root kits hook into the operating system's kernel and, therefore, operate underneath any authentication mechanism.

NEW QUESTION 184
The PRIMARY objective of a risk management program is to:

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

Answer: D

Explanation:

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

NEW QUESTION 185
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 187
The purpose of a corrective control is to:

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

Answer: C

Explanation:

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

NEW QUESTION 189
When implementing security controls, an information security manager must PRIMARILY focus on:

A. minimizing operational impact
B. eliminating all vulnerabilitie
C. usage by similar organization
D. certification from a third part

Answer: A

Explanation:

Security controls must be compatible with business needs. It is not feasible to eliminate all vulnerabilities. Usage by similar organizations does not guarantee that controls are adequate. Certification by a third party is important, but not a primary concern.

NEW QUESTION 191
When a significant security breach occurs, what should be reported FIRST to senior management?

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

Answer: B

Explanation:

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

NEW QUESTION 192
In a business impact analysis, the value of an information system should be based on the overall cost:

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

Answer: C

Explanation:

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

NEW QUESTION 195
When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

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

Answer: B

Explanation:

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

NEW QUESTION 200
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 205
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 210
Which two components PRIMARILY must be assessed in an effective risk analysis?

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

Answer: B

Explanation:

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

NEW QUESTION 213
Identification and prioritization of business risk enables project managers to:

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

Answer: C

Explanation:

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

NEW QUESTION 215
Which of the following is the MOST appropriate use of gap analysis?

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

Answer: D

Explanation:

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

NEW QUESTION 216
The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

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

Answer: B

Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

NEW QUESTION 220
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 225
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 227
Who can BEST advocate the development of and ensure the success of an information security program?

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

Answer: C

Explanation:

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

NEW QUESTION 229
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 231
When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 236
A test plan to validate the security controls of a new system should be developed during which phase of the project?

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

Answer: C

Explanation:

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

NEW QUESTION 241
An information security program should be sponsored by:

A. infrastructure managemen
B. the corporate audit departmen
C. key business process owner
D. information security managemen

Answer: C

Explanation:

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

NEW QUESTION 245
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

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

Answer: B

Explanation:

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

NEW QUESTION 250
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 254
A digital signature using a public key infrastructure (PKI) will:

A. not ensure the integrity of a messag
B. rely on the extent to which the certificate authority (CA) is truste
C. require two parties to the message exchang
D. provide a high level of confidentialit

Answer: B

Explanation:

The certificate authority (CA) is a trusted third party that attests to the identity of the
signatory, and reliance will be a function of the level of trust afforded the CA. A digital signature would provide a level of assurance of message integrity, but it is a three-party exchange, including the CA. Digital signatures do not require encryption of the message in order to preserve confidentiality.

NEW QUESTION 258
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

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

Answer: A

Explanation:

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

NEW QUESTION 262
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 267
A border router should be placed on which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 269
At what stage of the applications development process would encryption key management initially be addressed?

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

Answer: A

Explanation:

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

NEW QUESTION 270
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

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

Answer: A

Explanation:

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

NEW QUESTION 274
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

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

Answer: D

Explanation:

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

NEW QUESTION 278
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 281
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 283
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 286
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 290
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 292
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. invite an external consultant to create the security strateg
B. allocate budget based on best practice
C. benchmark similar organization
D. define high-level business security requirement

Answer: D

Explanation:

All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements

should precede the others because the implementation should be based on those security requirements.

NEW QUESTION 297
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

A. calculating the residual ris
B. enforcing the security standar
C. redesigning the system chang
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 299
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

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

Answer: B

Explanation:

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

NEW QUESTION 300
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A. Authentication
B. Encryption
C. Prohibit employees from copying data to l)SB devices
D. Limit the use of USB devices

Answer: B

Explanation:

Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

NEW QUESTION 303
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

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

Answer: C

Explanation:

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

NEW QUESTION 305
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the syste
B. implement multifactor authenticatio
C. rebuild the system from the original installation mediu
D. disconnect the mail server from the networ

Answer: C

Explanation:

Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

NEW QUESTION 306
Which of the following is the MOST effective type of access control?

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

Answer: B

Explanation:

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

NEW QUESTION 307
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 312
The MOST important success factor to design an effective IT security awareness program is to:

A. customize the content to the target audienc
B. ensure senior management is represente
C. ensure that all the staff is traine
D. avoid technical content but give concrete example

Answer: A

Explanation:

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

NEW QUESTION 317
The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

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

Answer: C

Explanation:

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

NEW QUESTION 319

On which of the following should a firewall be placed?

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

Answer: D

Explanation:

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

NEW QUESTION 322
In an organization, information systems security is the responsibility of:

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

Answer: A

Explanation:

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

NEW QUESTION 323
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

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

Answer: B

Explanation:

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

NEW QUESTION 328
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 329
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

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

Answer: A

Explanation:

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

NEW QUESTION 332
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. ensure the confidentiality of sensitive materia
B. provide a high assurance of identit
C. allow deployment of the active director
D. implement secure sockets layer (SSL) encryptio

Answer: B

Explanation:

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

NEW QUESTION 334
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

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

Answer: B

Explanation:

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

NEW QUESTION 336
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 338
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

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

Answer: A

Explanation:

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

NEW QUESTION 341
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 344
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 345
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 348
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

A. Encryption
B. Digital certificate
C. Digital signature
D. I lashing algorithm

Answer: A

Explanation:

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

NEW QUESTION 351
An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RI P) is the:

A. references from other organization
B. past experience of the engagement tea
C. sample deliverabl
D. methodology used in the assessmen

Answer: D

Explanation:

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

NEW QUESTION 356
Which of the following is the BEST indicator that an effective security control is built into an organization?

A. The monthly service level statistics indicate a minimal impact from security issue
B. The cost of implementing a security control is less than the value of the asset
C. The percentage of systems that is compliant with security standard
D. The audit reports do not reflect any significant findings on securit

Answer: A

Explanation:

The best indicator of effective security control is the evidence of little disruption to business operations. Choices B, C and D can support this evidence, but are supplemental to choice A.

NEW QUESTION 357
The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager

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

Answer: C

Explanation:

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

NEW QUESTION 359
The MOST important reason for formally documenting security procedures is to ensure:

A. processes are repeatable and sustainabl
B. alignment with business objective
C. auditability by regulatory agencie
D. objective criteria for the application of metric

Answer: A

Explanation:

Without formal documentation, it would be difficult to ensure that security processes are performed in the proper manner every time that they are performed. Alignment with business objectives is not a function of formally documenting security procedures. Processes should not be formally documented merely to satisfy an audit requirement. Although potentially useful in the development of metrics, creating formal documentation to assist in the creation of metrics is a secondary objective.

NEW QUESTION 361
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

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

Answer: B

Explanation:

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

NEW QUESTION 366
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

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

Answer: A

Explanation:

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

NEW QUESTION 370
Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

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

Answer: B

Explanation:

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

NEW QUESTION 372
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 373
Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

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

Answer: D

Explanation:

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

NEW QUESTION 375
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 377
To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

A. create a separate account for the programmer as a power use
B. log all of the programmers' activity for review by superviso
C. have the programmer sign a letter accepting full responsibilit
D. perform regular audits of the applicatio

Answer: B

Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers' actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

NEW QUESTION 381
In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

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

Answer: B

Explanation:

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

NEW QUESTION 384
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

A. Review of various security models
B. Discussion of how to construct strong passwords
C. Review of roles that have privileged access
D. Discussion of vulnerability assessment results

Answer: B

Explanation:

All new employees will need to understand techniques for the construction of strong passwords. The other choices would not be applicable to general staff employees.

NEW QUESTION 386
Data owners will determine what access and authorizations users will have by:

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

Answer: D

Explanation:

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

NEW QUESTION 389
Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

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

Answer: B

Explanation:

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

NEW QUESTION 392
To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

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

Answer: C

Explanation:

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

operations but does not get involved at the procedural level.

NEW QUESTION 395
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 398
The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

A. identifying vulnerabilities in the syste
B. sustaining the organization's security postur
C. the existing systems that will be affecte
D. complying with segregation of dutie

Answer: B

Explanation:

It is important to maintain the organization's security posture at all times. The focus should not be confined to the new system being developed or acquired, or to the existing systems in use. Segregation of duties is only part of a solution to improving the security of the systems, not the primary reason to involve security in the systems development life cycle (SDLC).

NEW QUESTION 403
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 404
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

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

Answer: C

Explanation:

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

NEW QUESTION 408
Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

A. User ad hoc reporting is not logged
B. Network traffic is through a single switch
C. Operating system (OS) security patches have not been applied
D. Database security defaults to ERP settings

Answer:

C

Explanation:

The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security- weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

NEW QUESTION 411
A critical component of a continuous improvement program for information security is:

A. measuring processes and providing feedbac
B. developing a service level agreement (SLA) for securit
C. tying corporate security standards to a recognized international standar
D. ensuring regulatory complianc

Answer: A

Explanation:

If an organization is unable to take measurements that will improve the level of its safety program. then continuous improvement is not possible. Although desirable, developing a service level agreement (SLA) for security, tying corporate security standards to a recognized international standard and ensuring regulatory compliance are not critical components for a continuous improvement program.

NEW QUESTION 413
In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

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

Answer: C

Explanation:

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

NEW QUESTION 416
The PRIMARY focus of the change control process is to ensure that changes are:

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

Answer: A

Explanation:

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

NEW QUESTION 419
Security policies should be aligned MOST closely with:

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

Answer: B

Explanation:

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

NEW QUESTION 423
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

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

Answer: B

Explanation:

Security software will generally have a well-controlled process for applying patches, backing up files and upgrading hardware. The greatest risk occurs when access rules are changed since they are susceptible to being opened up too much, which can result in the creation of a security exposure.

NEW QUESTION 428
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

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

Answer: B

Explanation:

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

NEW QUESTION 432
What is the MOST important success factor in launching a corporate information security awareness program?

A. Adequate budgetary support
B. Centralized program management
C. Top-down approach
D. Experience of the awareness trainers

Answer: C

Explanation:

Senior management support will provide enough resources and will focus attention to the program: training should start at the top levels to gain support and sponsorship. Funding is not a primary concern. Centralized management does not provide sufficient support. Trainer experience, while important, is not the primary success factor.

NEW QUESTION 433
Which of the following documents would be the BES T reference to determine whether access control mechanisms are appropriate for a critical application?

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

Answer: C

Explanation:

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

NEW QUESTION 436
An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

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

Answer: A

Explanation:

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

NEW QUESTION 439
The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

A. system develope

B. information security manage
C. steering committe
D. system data owne

Answer: D

Explanation:

Data owners are the most knowledgeable of the security needs of the business application for which they are responsible. The system developer, security manager and system custodian will have specific knowledge on limited areas but will not have full knowledge of the business issues that affect the level of security required. The steering committee does not perform at that level of detail on the operation.

NEW QUESTION 440
The BEST way to ensure that an external service provider complies with organizational security policies is to:

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

Answer: D

Explanation:

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

NEW QUESTION 444
The implementation of continuous monitoring controls is the BEST option where:

A. incidents may have a high impact and frequency
B. legislation requires strong information security controls
C. incidents may have a high impact but low frequency
D. Electronic commerce is a primary business driver

Answer: A

Explanation:

Continuous monitoring control initiatives are expensive, so they have to be used in areas where the risk is at its greatest level. These areas are the ones with high impact and high frequency of occurrence. Regulations and legislations that require tight IT security measures focus on requiring organizations to establish an IT security governance structure that manages IT security with a risk-based approach, so each organization decides which kinds of controls are implemented. Continuous monitoring is not necessarily a requirement. Measures such as contingency planning are commonly used when incidents rarely happen but have a high impact each time they happen. Continuous monitoring is unlikely to be necessary. Continuous control monitoring initiatives are not needed in all electronic commerce environments. There are some electronic commerce environments where the impact of incidents is not high enough to support the implementation of this kind of initiative.

NEW QUESTION 449
Managing the life cycle of a digital certificate is a role of a(n):

A. system administrato
B. security administrato
C. system develope
D. independent trusted sourc

Answer: D

Explanation:

Digital certificates must be managed by an independent trusted source in order to maintain trust in their authenticity. The other options are not necessarily entrusted with this capability.

NEW QUESTION 450
Successful social engineering attacks can BEST be prevented through:

A. preemployment screenin
B. close monitoring of users' access pattern
C. periodic awareness trainin
D. efficient termination procedure

Answer: C

Explanation:

Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

NEW QUESTION 453

.....

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