

Isaca

Exam Questions CISM

Certified Information Security Manager



NEW QUESTION 1

When an organization is implementing an information security governance program, its board of directors should be responsible for:

- A. drafting information security policies
- B. reviewing training and awareness program
- C. setting the strategic direction of the program
- D. auditing for compliance

Answer: C

Explanation:

A board of directors should establish the strategic direction of the program to ensure that it is in sync with the company's vision and business goals. The board must incorporate the governance program into the overall corporate business strategy. Drafting information security policies is best fulfilled by someone such as a security manager with the expertise to bring balance, scope and focus to the policies. Reviewing training and awareness programs may best be handled by security management and training staff to ensure that the training is on point and follows best practices. Auditing for compliance is best left to the internal and external auditors to provide an objective review of the program and how it meets regulatory and statutory compliance.

NEW QUESTION 2

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

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

Answer: D

Explanation:

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

NEW QUESTION 3

What would be the MOST significant security risks when using wireless local area network (LAN) technology?

- A. Man-in-the-middle attack
- B. Spoofing of data packets
- C. Rogue access point
- D. Session hijacking

Answer: C

Explanation:

A rogue access point masquerades as a legitimate access point. The risk is that legitimate users may connect through this access point and have their traffic monitored. All other choices are not dependent on the use of a wireless local area network (LAN) technology.

NEW QUESTION 4

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 5

Which of the following is MOST likely to be discretionary?

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

Answer: C

Explanation:

Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control; as such, they are discretionary.

NEW QUESTION 6

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

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

Answer: D

Explanation:

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

NEW QUESTION 7

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

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 (KRI) 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 (KRI) 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 9

Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

- A. The security officer
- B. Senior management
- C. The end user
- D. The custodian

Answer: B

Explanation:

Routine administration of all aspects of security is delegated, but top management must retain overall responsibility. The security officer supports and implements information security for senior management. The end user does not perform categorization. The custodian supports and implements information security measures as directed.

NEW QUESTION 10

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 10

Investments in information security technologies should be based on:

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

Answer: B

Explanation:

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

NEW QUESTION 14

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 16

Information security governance is PRIMARILY driven by:

- A. technology constraint
- B. regulatory requirement
- C. litigation potential
- D. business strategy

Answer: D

Explanation:

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

NEW QUESTION 21

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

- A. aligned with the IT strategic plan
- B. based on the current rate of technological change
- C. three-to-five years for both hardware and software
- D. aligned with the business strategy

Answer: D

Explanation:

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

NEW QUESTION 23

Who should be responsible for enforcing access rights to application data?

- A. Data owners
- B. Business process owners
- C. The security steering committee
- D. Security administrators

Answer: D

Explanation:

As custodians, security administrators are responsible for enforcing access rights to data. Data owners are responsible for approving these access rights. Business process owners are sometimes the data owners as well, and would not be responsible for enforcement. The security steering committee would not be responsible for enforcement.

NEW QUESTION 26

What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

- A. Risk assessment report
- B. Technical evaluation report
- C. Business case
- D. Budgetary requirements

Answer: C

Explanation:

The information security manager needs to prioritize the controls based on risk management and the requirements of the organization. The information security manager must look at the costs of the various controls and compare them against the benefit the organization will receive from the security solution. The information security manager needs to have knowledge of the development of business cases to illustrate the costs and benefits of the various controls. All other choices are supplemental.

NEW QUESTION 30

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

- A. organizational risk
- 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 35

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 40

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 45

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

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

Answer: D

Explanation:

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

NEW QUESTION 47

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

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

Answer: C

Explanation:

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

NEW QUESTION 48

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

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

Answer: A

Explanation:

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

NEW QUESTION 53

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

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

Answer: B

Explanation:

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

NEW QUESTION 54

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

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

Answer: C

Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

NEW QUESTION 58

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

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

Answer: B

Explanation:

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

NEW QUESTION 61

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 64

To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

- A. review the functionalities and implementation requirements of the solution
- B. review comparison reports of tool implementation in peer companies
- C. provide examples of situations where such a tool would be useful
- D. substantiate the investment in meeting organizational need

Answer: D

Explanation:

Any investment must be reviewed to determine whether it is cost effective and supports the organizational strategy. It is important to review the features and functionalities provided by such a tool, and to provide examples of situations where the tool would be useful, but that comes after substantiating the investment and return on investment to the organization.

NEW QUESTION 65

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

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

Answer: C

Explanation:

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

NEW QUESTION 68

At what stage of the applications development process should the security department initially become involved?

- A. When requested
- B. At testing

- C. At programming
- D. At detail requirements

Answer: D

Explanation:

Information security has to be integrated into the requirements of the application's design. It should also be part of the information security governance of the organization. The application owner may not make a timely request for security involvement. It is too late during systems testing, since the requirements have already been agreed upon. Code reviews are part of the final quality assurance process.

NEW QUESTION 70

Acceptable levels of information security risk should be determined by:

- A. legal counsel
- B. security management
- C. external auditor
- D. the steering committee

Answer: D

Explanation:

Senior management, represented in the steering committee, has ultimate responsibility for determining what levels of risk the organization is willing to assume. Legal counsel, the external auditors and security management are not in a position to make such a decision.

NEW QUESTION 73

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- A. establishing a periodic risk assessment
- B. promoting regulatory requirements
- C. developing a business case
- D. developing effective metrics

Answer: C

Explanation:

Business case development, including a cost-benefit analysis, will be most persuasive to management. A risk assessment may be included in the business case, but by itself will not be as effective in gaining management support. Informing management of regulatory requirements may help gain support for initiatives, but given that more than half of all organizations are not in compliance with regulations, it is unlikely to be sufficient in many cases. Good metrics which provide assurance that initiatives are meeting organizational goals will also be useful, but are insufficient in gaining management support.

NEW QUESTION 76

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

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

Answer: D

Explanation:

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

NEW QUESTION 81

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

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

Answer: B

Explanation:

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

NEW QUESTION 82

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

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

Answer: D

Explanation:

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

NEW QUESTION 85

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

- A. develop a security architecture
- B. install a network intrusion detection system (NIDS) and prepare a list of attacks
- C. develop a network security policy
- D. conduct a risk assessment

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 89

A good privacy statement should include:

- A. notification of liability on accuracy of information
- B. notification that information will be encrypted
- C. what the company will do with information it collects
- D. a description of the information classification process

Answer: C

Explanation:

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

NEW QUESTION 92

Retention of business records should PRIMARILY be based on:

- A. business strategy and direction
- B. regulatory and legal requirements
- C. storage capacity and longevity
- D. business case and value analysis

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 94

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 97

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 101

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

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

Answer: A

Explanation:

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

NEW QUESTION 106

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

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

Answer: D

Explanation:

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

NEW QUESTION 110

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

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

Answer: D

Explanation:

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

NEW QUESTION 115

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 119

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

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

Answer: C

Explanation:

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

NEW QUESTION 122

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 policy
- B. data privacy policy where data are collected
- C. data privacy policy of the headquarters' country
- D. data privacy directive applicable globally

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 127

Which of the following situations would MOST inhibit the effective implementation of security governance:

- A. The complexity of technology
- B. Budgetary constraints
- C. Conflicting business priorities
- D. High-level sponsorship

Answer: D

Explanation:

The need for senior management involvement and support is a key success factor for the implementation of appropriate security governance. Complexity of technology, budgetary constraints and conflicting business priorities are realities that should be factored into the governance model of the organization, and should not be regarded as inhibitors.

NEW QUESTION 128

The MOST important component of a privacy policy is:

- A. notification
- B. warranty
- C. liability
- D. geographic coverage

Answer: A

Explanation:

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

NEW QUESTION 131

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

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

Answer: B

Explanation:

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

NEW QUESTION 133

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

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

Answer: A

Explanation:

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

NEW QUESTION 137

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

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

Answer: D

Explanation:

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

NEW QUESTION 141

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

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

Answer: B

Explanation:

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

NEW QUESTION 144

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

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

Answer: B

Explanation:

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

NEW QUESTION 147

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

- A. annualized loss expectanc
- B. cost of an inciden
- C. asset valu
- D. implementation opportunity cost

Answer: C

Explanation:

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

NEW QUESTION 150

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 153

Which of the following authentication methods prevents authentication replay?

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

Answer: B

Explanation:

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

NEW QUESTION 155

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 160

Risk management programs are designed to reduce risk to:

- A. a level that is too small to be measurabl
- B. the point at which the benefit exceeds the expens
- C. a level that the organization is willing to accep
- D. a rate of return that equals the current cost of capita

Answer: C

Explanation:

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive.

To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

NEW QUESTION 164

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

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

Answer: B

Explanation:

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

NEW QUESTION 166

The BEST strategy for risk management is to:

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

Answer: B

Explanation:

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

NEW QUESTION 170

The MOST effective use of a risk register is to:

- A. identify risks and assign roles and responsibilities for mitigation
- B. identify threats and probabilities
- C. facilitate a thorough review of all IT-related risks on a periodic basis
- D. record the annualized financial amount of expected losses due to risk

Answer: C

Explanation:

A risk register is more than a simple list—it should be used as a tool to ensure comprehensive documentation, periodic review and formal update of all risk elements in the enterprise's IT and related organization. Identifying risks and assigning roles and responsibilities for mitigation are elements of the register. Identifying threats and probabilities are two elements that are defined in the risk matrix, as differentiated from the broader scope of content in, and purpose for, the risk register. While the annualized loss expectancy (ALE) should be included in the register, this quantification is only a single element in the overall risk analysis program.

NEW QUESTION 172

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

- A. hourly billing rate charged by the carrier
- B. value of the data transmitted over the network
- C. aggregate compensation of all affected business users
- 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 175

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

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

Answer:

C

Explanation:

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

NEW QUESTION 179

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

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

Answer: C

Explanation:

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

NEW QUESTION 180

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

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

Answer: A

Explanation:

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

NEW QUESTION 181

Phishing is BEST mitigated by which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 186

Risk acceptance is a component of which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 191

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

- A. Defining job roles
- B. Performing a risk assessment
- C. Identifying data owners
- D. Establishing data retention policies

Answer: C

Explanation:

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

NEW QUESTION 196

A risk management program would be expected to:

- A. remove all inherent risk
- B. maintain residual risk at an acceptable level
- C. implement preventive controls for every threat
- D. reduce control risk to zero

Answer: B

Explanation:

The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

NEW QUESTION 200

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

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

Answer: C

Explanation:

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

NEW QUESTION 204

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

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

Answer: D

Explanation:

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

NEW QUESTION 209

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

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

Answer: B

Explanation:

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

NEW QUESTION 210

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

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

D. Owner

Answer: D

Explanation:

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

NEW QUESTION 212

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

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

Answer: D

Explanation:

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

NEW QUESTION 213

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 engineering
- C. immediately advise senior management of the elevated risk
- D. increase monitoring activities to provide early detection of intrusion

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 218

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 219

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

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

Answer: C

Explanation:

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

NEW QUESTION 222

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 226

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

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

Answer: D

Explanation:

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

NEW QUESTION 231

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

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

Answer: B

Explanation:

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

NEW QUESTION 235

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 239

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 242

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

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

Answer: C

Explanation:

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

NEW QUESTION 245

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 246

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

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

Answer: B

Explanation:

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

NEW QUESTION 249

The PRIMARY objective of a risk management program is to:

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

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 250

The valuation of IT assets should be performed by:

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

Answer: D

Explanation:

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep

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

NEW QUESTION 252

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

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

Answer: D

Explanation:

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

NEW QUESTION 254

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 case 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 256

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

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

Answer: B

Explanation:

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

NEW QUESTION 261

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

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

Answer: D

Explanation:

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

NEW QUESTION 262

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

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

Answer:

C

Explanation:

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

NEW QUESTION 264

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

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

Answer: B

Explanation:

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

NEW QUESTION 268

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

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

Answer: B

Explanation:

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

NEW QUESTION 273

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

- A. minimizing operational impact
- B. eliminating all vulnerabilities
- C. usage by similar organizations
- D. certification from a third party

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 274

Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

- A. Annual loss expectancy (ALE) of incidents
- B. Frequency of incidents
- C. Total cost of ownership (TCO)
- D. Approved budget for the project

Answer: C

Explanation:

The total cost of ownership (TCO) would be the most relevant piece of information in that it would establish a cost baseline and it must be considered for the full life cycle of the control. Annual loss expectancy (ALE) and the frequency of incidents could help measure the benefit, but would have more of an indirect relationship as not all incidents may be mitigated by implementing a two-factor authentication system. The approved budget for the project may have no bearing on what the project may actually cost.

NEW QUESTION 278

An information security organization should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 279

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

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

Answer: C

Explanation:

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

NEW QUESTION 282

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

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

Answer: B

Explanation:

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

NEW QUESTION 287

In assessing risk, it is MOST essential to:

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

Answer: C

Explanation:

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

NEW QUESTION 292

A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

- A. Risk analysis results
- B. Audit report findings
- C. Penetration test results
- D. Amount of IT budget available

Answer: A

Explanation:

Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

NEW QUESTION 294

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 296

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

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

Answer: B

Explanation:

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

NEW QUESTION 297

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 298

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

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

Answer: D

Explanation:

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

NEW QUESTION 299

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

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

Answer: C

Explanation:

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

NEW QUESTION 304

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

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

Answer: A

Explanation:

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

NEW QUESTION 309

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

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

Answer: C

Explanation:

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

NEW QUESTION 313

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

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

Answer: B

Explanation:

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

NEW QUESTION 317

Which of the following guarantees that data in a file have not changed?

- A. Inspecting the modified date of the file
- B. Encrypting the file with symmetric encryption
- C. Using stringent access control to prevent unauthorized access
- D. Creating a hash of the file, then comparing the file hashes

Answer: D

Explanation:

A hashing algorithm can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

NEW QUESTION 321

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 325

An information security program should be sponsored by:

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

Answer: C

Explanation:

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

NEW QUESTION 326

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

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

Answer: C

Explanation:

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

NEW QUESTION 329

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

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

Answer: D

Explanation:

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

NEW QUESTION 332

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 333

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 338

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 339

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 344

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

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

Answer: B

Explanation:

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

NEW QUESTION 345

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

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

Answer: D

Explanation:

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

NEW QUESTION 348

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

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

Answer: A

Explanation:

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

NEW QUESTION 353

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 356

Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

- A. Strong authentication by password
- B. Encrypted hard drives
- C. Multifactor authentication procedures
- D. Network-based data backup

Answer: B

Explanation:

Encryption of the hard disks will prevent unauthorized access to the laptop even when the laptop is lost or stolen. Strong authentication by password can be bypassed by a determined hacker. Multifactor authentication can be bypassed by removal of the hard drive and insertion into another laptop. Network-based data backups do not prevent access but rather recovery from data loss.

NEW QUESTION 358

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

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

Answer: B

Explanation:

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

NEW QUESTION 362

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

- A. number of attacks blocked
- B. number of packets dropped
- C. average throughput rate
- D. number of firewall rules

Answer: A

Explanation:

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

NEW QUESTION 364

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

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

Answer: C

Explanation:

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

NEW QUESTION 365

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

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

Answer: D

Explanation:

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

NEW QUESTION 369

Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

- A. Regular review of access control lists
- B. Security guard escort of visitors
- C. Visitor registry log at the door
- D. A biometric coupled with a PIN

Answer: A

Explanation:

A review of access control lists is a detective control that will enable an information security manager to ensure that authorized persons are entering in compliance with corporate policy. Visitors accompanied by a guard will also provide assurance but may not be cost effective. A visitor registry is the next cost-effective control. A biometric coupled with a PIN will strengthen the access control; however, compliance assurance logs will still have to be reviewed.

NEW QUESTION 370

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

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

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 373

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 374

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

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

Answer: C

Explanation:

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

NEW QUESTION 377

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 381

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 dvice.

NEW QUESTION 384

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

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

Answer: C

Explanation:

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

NEW QUESTION 388

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

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

Answer: B

Explanation:

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

NEW QUESTION 389

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

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

Answer: C

Explanation:

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

NEW QUESTION 391

The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

- A. messages displayed at every login
- B. periodic security-related e-mail message
- C. an Intranet web site for information security
- D. circulating the information security policy

Answer: A

Explanation:

Login banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet web site does not force users to access it and read the information. Circulating the information security policy alone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

NEW QUESTION 392

Good information security standards should:

- A. define precise and unambiguous allowable limits
- B. describe the process for communicating violations
- C. address high-level objectives of the organization
- D. be updated frequently as new software is released

Answer: A

Explanation:

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

NEW QUESTION 394

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 issues
- 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 standards
- D. The audit reports do not reflect any significant findings on security

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 399

Security awareness training should be provided to new employees:

- A. on an as-needed basis
- B. during system user training

- C. before they have access to dat
- D. along with department staf

Answer: C

Explanation:

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

NEW QUESTION 403

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 405

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 410

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

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

Answer: B

Explanation:

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

NEW QUESTION 412

Good information security procedures should:

- A. define the allowable limits of behavio
- B. underline the importance of security governanc
- C. describe security baselines for each platfor
- D. be updated frequently as new software is release

Answer: D

Explanation:

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

NEW QUESTION 416

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

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

Answer: A

Explanation:

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

NEW QUESTION 417

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

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

Answer: A

Explanation:

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

NEW QUESTION 422

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

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

Answer: A

Explanation:

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

NEW QUESTION 427

What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

- A. all use weak encryptio
- B. are decrypted by the firewal
- C. may be quarantined by mail filter
- D. may be corrupted by the receiving mail serve

Answer: C

Explanation:

Often, mail filters will quarantine zip files that are password-protected since the filter (or the firewall) is unable to determine if the file contains malicious code. Many zip file products are capable of using strong encryption. Such files are not normally corrupted by the sending mail server.

NEW QUESTION 428

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 432

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

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

Answer: D

Explanation:

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

NEW QUESTION 434

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

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

Answer: A

Explanation:

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

NEW QUESTION 435

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

- A. set their accounts to expire in six months or less
- B. avoid granting system administration role
- C. ensure they successfully pass background check
- D. ensure their access is approved by the data owner

Answer: B

Explanation:

Contract personnel should not be given job duties that provide them with power user or other administrative roles that they could then use to grant themselves access to sensitive files. Setting expiration dates, requiring background checks and having the data owner assign access are all positive elements, but these will not prevent contract personnel from obtaining access to sensitive information.

NEW QUESTION 440

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 441

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

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

Answer: A

Explanation:

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

NEW QUESTION 445

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

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

Answer: C

Explanation:

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

NEW QUESTION 450

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

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

Answer: A

Explanation:

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

NEW QUESTION 451

What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

- A. Perform periodic penetration testing
- B. Establish minimum security baselines
- C. Implement vendor default settings
- D. Install a honeypot on the network

Answer: D

Explanation:

Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed sporadically. Vendor default settings are not effective.

NEW QUESTION 455

Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

- A. Security policies and procedures
- B. Annual self-assessment by management
- C. Security- steering committees
- D. Security awareness campaigns

Answer: C

Explanation:

Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self- assessment exercises are all good but do not exemplify the taking of ownership by management.

NEW QUESTION 460

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

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

Answer: D

Explanation:

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

NEW QUESTION 461

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

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

Answer: C

Explanation:

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

NEW QUESTION 463

Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

- A. Acceptable use policy
- B. Setting low mailbox limits
- C. User awareness training
- D. Taking disciplinary action

Answer: C

Explanation:

User awareness training would help in reducing the incidents of employees forwarding spam and chain e-mails since users would understand the risks of doing so and the impact on the organization's information system. An acceptable use policy, signed by employees, would legally address the requirements but merely having a policy is not the best measure. Setting low mailbox limits and taking disciplinary action are a reactive approach and may not help in obtaining proper support from employees.

NEW QUESTION 467

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

- A. system developer
- B. information security manager
- C. steering committee
- D. system data owner

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 468

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISM Practice Exam Features:

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

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