

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

Which of the following is MOST important to understand when developing a meaningful information security strategy?

- A. Regulatory environment
- B. International security standards
- C. Organizational risks
- D. Organizational goals

Answer: D

Explanation:

Alignment of security with business objectives requires an understanding of what an organization is trying to accomplish. The other choices are all elements that must be considered, but their importance is secondary and will vary depending on organizational goals.

NEW QUESTION 3

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

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 5

An outcome of effective security governance is:

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

Answer: B

Explanation:

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

NEW QUESTION 6

Successful implementation of information security governance will FIRST require:

- A. security awareness trainin
- B. updated security policie
- C. a computer incident management tea
- D. a security architectur

Answer: B

Explanation:

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

NEW QUESTION 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 resolutio
- B. ensure that senior management provides authority for security to address the issue
- C. insist that managers or units not in agreement with the security solution accept the ris
- D. refer the issues to senior management along with any security recommendation

Answer: D

Explanation:

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

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

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

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

Answer: A

Explanation:

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

NEW QUESTION 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 11

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 15

The PRIMARY objective of a security steering group is to:

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

Answer: B

Explanation:

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

NEW QUESTION 19

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 20

A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

- A. meet with stakeholders to decide how to compl
- B. analyze key risks in the compliance proces
- C. assess whether existing controls meet the regulatio
- D. update the existing security/privacy polic

Answer: C

Explanation:

If the organization is in compliance through existing controls, the need to perform other work related to the regulation is not a priority. The other choices are appropriate and important; however, they are actions that are subsequent and will depend on whether there is an existing control gap.

NEW QUESTION 25

The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

- A. head of internal audi
- B. chief operations officer (COO).
- C. chief technology officer (CTO).
- D. legal counse

Answer: B

Explanation:

The chief information security officer (CISO) should ideally report to as high a level within the organization as possible. Among the choices given, the chief operations officer (COO) would have not only the appropriate level but also the knowledge of day-to-day operations. The head of internal audit and legal counsel would make good secondary choices, although they would not be as knowledgeable of the operations. Reporting to the chief technology officer (CTO) could become problematic as the CTO's goals for the infrastructure might, at times, run counter to the goals of information security.

NEW QUESTION 26

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

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

Answer: D

Explanation:

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

NEW QUESTION 29

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

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

Answer: A

Explanation:

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

NEW QUESTION 33

Which of the following is an advantage of a centralized information security organizational structure?

- A. It is easier to promote security awarenes
- B. It is easier to manage and contro
- C. It is more responsive to business unit need
- D. It provides a faster turnaround for security request

Answer: B

Explanation:

It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization. Decentralization allows you to use field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

NEW QUESTION 36

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 38

Investment in security technology and processes should be based on:

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

Answer: A

Explanation:

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

NEW QUESTION 41

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

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

Answer: B

Explanation:

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

NEW QUESTION 46

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 48

Which of the following are likely to be updated MOST frequently?

- A. Procedures for hardening database servers
- B. Standards for password length and complexity

- C. Policies addressing information security governance
- D. Standards for document retention and destruction

Answer: A

Explanation:

Policies and standards should generally be more static and less subject to frequent change. Procedures on the other hand, especially with regard to the hardening of operating systems, will be subject to constant change; as operating systems change and evolve, the procedures for hardening will have to keep pace.

NEW QUESTION 50

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

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

Answer: A

Explanation:

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

NEW QUESTION 53

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 57

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

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

Answer: B

Explanation:

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

NEW QUESTION 60

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

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

Answer: A

Explanation:

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

NEW QUESTION 61

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 65

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 70

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

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

Answer: A

Explanation:

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

NEW QUESTION 72

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

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

Answer: A

Explanation:

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

NEW QUESTION 75

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 78

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 80

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 83

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

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

Answer: A

Explanation:

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

NEW QUESTION 88

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

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

Answer: A

Explanation:

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

NEW QUESTION 91

While implementing information security governance an organization should FIRST:

- A. adopt security standard
- B. determine security baseline
- C. define the security strategy
- D. establish security policies

Answer: C

Explanation:

The first step in implementing information security governance is to define the security strategy based on which security baselines are determined. Adopting

suitable security-standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

NEW QUESTION 95

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

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

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 99

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 104

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 105

Who is ultimately responsible for the organization's information?

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

Answer: C

Explanation:

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

NEW QUESTION 109

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 112

A good privacy statement should include:

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

Answer: C

Explanation:

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

NEW QUESTION 115

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

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

Answer: C

Explanation:

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

NEW QUESTION 119

Which of the following is MOST important in developing a security strategy?

- A. Creating a positive business security environment
- B. Understanding key business objectives
- C. Having a reporting line to senior management
- D. Allocating sufficient resources to information security

Answer: B

Explanation:

Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

NEW QUESTION 121

Retention of business records should PRIMARILY be based on:

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

Answer: B

Explanation:

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

NEW QUESTION 124

To achieve effective strategic alignment of security initiatives, it is important that:

- A. Steering committee leadership be selected by rotatio
- B. Inputs be obtained and consensus achieved between the major organizational unit
- C. The business strategy be updated periodical
- D. Procedures and standards be approved by all departmental head

Answer: B

Explanation:

It is important to achieve consensus on risks and controls, and obtain inputs from various organizational entities since security needs to be aligned to the needs of the organization. Rotation of steering committee leadership does not help in achieving strategic alignment. Updating business strategy does not lead to strategic alignment of security initiatives. Procedures and standards need not be approved by all departmental heads

NEW QUESTION 126

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

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

Answer: C

Explanation:

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

NEW QUESTION 131

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

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

Answer: A

Explanation:

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

NEW QUESTION 136

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 strateg

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 137

What is the MOST important factor in the successful implementation of an enterprise wide information security program?

- A. Realistic budget estimates
- B. Security awareness
- C. Support of senior management
- D. Recalculation of the work factor

Answer: C

Explanation:

Without the support of senior management, an information security program has little chance of survival. A company's leadership group, more than any other group, will more successfully drive the program. Their authoritative position in the company is a key factor. Budget approval, resource commitments, and companywide participation also require the buy-in from senior management. Senior management is responsible for providing an adequate budget and the necessary resources. Security awareness is important, but not the most important factor. Recalculation of the work factor is a part of risk management.

NEW QUESTION 140

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 144

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 147

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

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

Answer: A

Explanation:

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

NEW QUESTION 152

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 153

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 156

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

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

Answer: B

Explanation:

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

NEW QUESTION 157

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. Baselineing against the information security metrics will be considered later in the process.

NEW QUESTION 160

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

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

Answer: B

Explanation:

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

NEW QUESTION 165

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 166

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

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

Answer: B

Explanation:

New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support. Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly,

developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

NEW QUESTION 169

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

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

Answer: D

Explanation:

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

NEW QUESTION 173

Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

- A. assessing the frequency of incident
- B. quantifying the cost of control failure
- C. calculating return on investment (ROD projection)
- D. comparing spending against similar organization

Answer: C

Explanation:

Calculating the return on investment (ROD) will most closely align security with the impact on the bottom line. Frequency and cost of incidents are factors that go into determining the impact on the business but, by themselves, are insufficient. Comparing spending against similar organizations can be problematic since similar organizations may have different business goals and appetites for risk.

NEW QUESTION 177

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 178

Which of the following should be included in an annual information security budget that is submitted for management approval?

- A. A cost-benefit analysis of budgeted resources
- B. All of the resources that are recommended by the business
- C. Total cost of ownership (TCO)
- D. Baseline comparisons

Answer: A

Explanation:

A brief explanation of the benefit of expenditures in the budget helps to convey the context of how the purchases that are being requested meet goals and objectives, which in turn helps build credibility for the information security function or program. Explanations of benefits also help engage senior management in the support of the information security program. While the budget should consider all inputs and recommendations that are received from the business, the budget that is ultimately submitted to management for approval should include only those elements that are intended for purchase. TCO may be requested by management and may be provided in an addendum to a given purchase request, but is not usually included in an annual budget. Baseline comparisons (cost comparisons with other companies or industries) may be useful in developing a budget or providing justification in an internal review for an individual purchase, but would not be included with a request for budget approval.

NEW QUESTION 180

Information security should be:

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

Answer: B

Explanation:

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

NEW QUESTION 184

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

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

Answer: C

Explanation:

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

NEW QUESTION 187

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

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

Answer: A

Explanation:

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

NEW QUESTION 190

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

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

Answer: C

Explanation:

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

NEW QUESTION 193

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

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

Answer: D

Explanation:

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

NEW QUESTION 195

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 197

Which of the following would be the MOST important goal of an information security governance program?

- A. Review of internal control mechanisms
- B. Effective involvement in business decision making
- C. Total elimination of risk factors
- D. Ensuring trust in data

Answer: D

Explanation:

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true. Involvement in decision making is important only to ensure business data integrity so that data can be trusted.

NEW QUESTION 202

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

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

Answer: C

Explanation:

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

NEW QUESTION 206

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 210

Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- A. Include security responsibilities in the job description
- B. Require the administrator to obtain security certification
- C. Train the system administrator on penetration testing and vulnerability assessment
- D. Train the system administrator on risk assessment

Answer: A

Explanation:

The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

NEW QUESTION 213

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

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

Answer: C

Explanation:

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

NEW QUESTION 218

Which of the following should be determined while defining risk management strategies?

- A. Risk assessment criteria
- B. Organizational objectives and risk appetite
- C. IT architecture complexity
- D. Enterprise disaster recovery plans

Answer: B

Explanation:

While defining risk management strategies, one needs to analyze the organization's objectives and risk appetite and define a risk management framework based on this analysis. Some organizations may accept known risks, while others may invest in and apply mitigation controls to reduce risks. Risk assessment criteria would become part of this framework, but only after proper analysis. IT architecture complexity and enterprise disaster recovery plans are more directly related to assessing risks than defining strategies.

NEW QUESTION 220

Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

- A. More uniformity in quality of service
- B. Better adherence to policies
- C. Better alignment to business unit needs
- D. More savings in total operating costs

Answer: C

Explanation:

Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

NEW QUESTION 224

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

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

Answer: B

Explanation:

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

NEW QUESTION 225

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

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

Answer: C

Explanation:

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

NEW QUESTION 227

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

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

Answer: C

Explanation:

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

NEW QUESTION 228

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 231

Who should drive the risk analysis for an organization?

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

Answer: B

Explanation:

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

NEW QUESTION 235

Information security projects should be prioritized on the basis of:

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

Answer: AB

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

NEW QUESTION 237

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

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

Answer: C

Explanation:

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

NEW QUESTION 242

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 245

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

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

Answer: B

Explanation:

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

NEW QUESTION 246

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

- A. implement stronger control
- B. conduct periodic awareness trainin
- C. actively monitor operation
- D. gain the endorsement of executive managemen

Answer: D

Explanation:

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

NEW QUESTION 247

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

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

Answer: B

Explanation:

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

NEW QUESTION 249

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

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

Answer: D

Explanation:

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

NEW QUESTION 252

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 256

To determine the selection of controls required to meet business objectives, an information security manager should:

- A. prioritize the use of role-based access control
- B. focus on key control
- C. restrict controls to only critical application
- D. focus on automated control

Answer: B

Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

NEW QUESTION 258

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 261

One way to determine control effectiveness is by determining:

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

Answer: C

Explanation:

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

NEW QUESTION 263

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- A. Recover)' time objective (RTO)
- B. Maximum tolerable outage (MTO)
- C. Recovery point objectives (RPOs)
- D. Services delivery objectives (SDOs)

Answer: A

Explanation:

Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

NEW QUESTION 266

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 271

The value of information assets is BEST determined by:

- A. individual business manager
- B. business systems analyst
- C. information security management
- D. industry averages benchmarking

Answer: A

Explanation:

Individual business managers are in the best position to determine the value of information assets since they are most knowledgeable of the assets' impact on the business. Business systems developers and information security managers are not as knowledgeable regarding the impact on the business. Peer companies' industry averages do not necessarily provide detailed enough information nor are they as relevant to the unique aspects of the business.

NEW QUESTION 274

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 278

Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

- A. Disclosure of personal information
- B. Sufficient coverage of the insurance policy for accidental losses
- C. Intrinsic value of the data stored on the equipment
- D. Replacement cost of the equipment

Answer: C

Explanation:

When mobile equipment is lost or stolen, the information contained on the equipment matters most in determining the impact of the loss. The more sensitive the information, the greater the liability. If staff carries mobile equipment for business purposes, an organization must develop a clear policy as to what information should be kept on the equipment and for what purpose. Personal information is not defined in the question as the data that were lost. Insurance may be a relatively smaller issue as compared with information theft or opportunity loss, although insurance is also an important factor for a successful business. Cost of equipment would be a less important issue as compared with other choices.

NEW QUESTION 281

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 286

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 287

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

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

Answer: A

Explanation:

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

NEW QUESTION 289

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 spotlight 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 294

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 297

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 301

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

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

Answer: D

Explanation:

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

NEW QUESTION 303

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 304

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 308

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

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

Answer: A

Explanation:

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

NEW QUESTION 310

A successful risk management program should lead to:

- A. optimization of risk reduction efforts against cost
- B. containment of losses to an annual budgeted amount
- C. identification and removal of all man-made threat
- D. elimination or transference of all organizational risk

Answer: A

Explanation:

Successful risk management should lead to a breakeven point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, while losses cannot be budgeted in advance with absolute certainty.

NEW QUESTION 311

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 313

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 317

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

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

Answer: B

Explanation:

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

NEW QUESTION 321

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 324

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

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

Answer: B

Explanation:

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

NEW QUESTION 328

The MOST important function of a risk management program is to:

- A. quantify overall risk
- B. minimize residual risk
- C. eliminate inherent risk
- D. maximize the sum of all annualized loss expectancies (ALEs).

Answer: B

Explanation:

A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred; this is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

NEW QUESTION 331

A risk mitigation report would include recommendations for:

- A. assessment
- B. acceptance
- C. evaluation
- D. quantification

Answer: B

Explanation:

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

NEW QUESTION 333

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

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

Answer: B

Explanation:

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

NEW QUESTION 334

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 339

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

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

Answer: A

Explanation:

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

NEW QUESTION 341

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 345

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

- A. Business impact analysis (BIA)
- B. Penetration testing
- C. Audit and review
- D. Threat analysis

Answer: B

Explanation:

Penetration testing focuses on identifying vulnerabilities. None of the other choices would identify vulnerabilities introduced by changes.

NEW QUESTION 347

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 349

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

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

Answer: B

Explanation:

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

security function.

NEW QUESTION 351

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

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

Answer: D

Explanation:

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

NEW QUESTION 353

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

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

Answer: C

Explanation:

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

NEW QUESTION 356

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

- A. cost of protection is in proportion to sensitivity
- B. highly sensitive assets are protected
- C. cost of controls is minimized
- D. countermeasures are proportional to risk

Answer: D

Explanation:

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

NEW QUESTION 359

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- A. ensure the provider is made liable for losses
- B. recommend not renewing the contract upon expiration
- C. recommend the immediate termination of the contract
- D. determine the current level of security

Answer: D

Explanation:

It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

NEW QUESTION 362

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 367

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

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

Answer: A

Explanation:

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

NEW QUESTION 368

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 373

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

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

Answer: D

Explanation:

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

NEW QUESTION 375

The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

- A. sales department
- B. database administrator
- C. chief information officer (CIO).
- D. head of the sales department

Answer: D

Explanation:

The owner of the information asset should be the person with the decision-making power in the department deriving the most benefit from the asset. In this case, it would be the head of the sales department. The organizational unit cannot be the owner of the asset because that removes personal responsibility. The database administrator is a custodian. The chief information officer (CIO) would not be an owner of this database because the CTO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

NEW QUESTION 380

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

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

Answer: A

Explanation:

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

NEW QUESTION 382

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

- A. organizational requirement
- B. information systems requirement
- C. information security requirement
- D. international standard

Answer: A

Explanation:

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

NEW QUESTION 384

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

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

Answer: A

Explanation:

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

NEW QUESTION 386

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

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

Answer: D

Explanation:

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

NEW QUESTION 391

A risk assessment should be conducted:

- A. once a year for each business process and subproces
- B. every three to six months for critical business processe
- C. by external parties to maintain objectivit
- D. annually or whenever there is a significant chang

Answer: D

Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address

significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

NEW QUESTION 394

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

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

Answer: B

Explanation:

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

NEW QUESTION 396

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

- A. minimizing operational impact
- B. eliminating all vulnerabilities
- C. usage by similar organization
- 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 401

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

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

Answer: C

Explanation:

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

NEW QUESTION 404

Information security managers should use risk assessment techniques to:

- A. justify selection of risk mitigation strategies
- B. maximize the return on investment (ROI)
- C. provide documentation for auditors and regulators
- D. quantify risks that would otherwise be subjective

Answer: A

Explanation:

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

NEW QUESTION 405

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

- A. of recovery
- B. to recreate
- C. if unavailable
- D. of emergency operation

Answer: C

Explanation:

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

NEW QUESTION 407

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 409

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

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

Answer: B

Explanation:

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

NEW QUESTION 413

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISM Practice Exam Features:

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

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