

CISM Dumps

Certified Information Security Manager

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



NEW QUESTION 1

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

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

Answer: B

Explanation:

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

NEW QUESTION 2

Which of the following is responsible for legal and regulatory liability?

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

Answer: C

Explanation:

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

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: C

Explanation:

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

NEW QUESTION 5

Which of the following is MOST likely to be discretionary?

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

Answer: C

Explanation:

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

NEW QUESTION 6

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

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

Answer: D

Explanation:

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

NEW QUESTION 7

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 8

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 9

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

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 10

When a security standard conflicts with a business objective, the situation should be resolved by:

- A. changing the security standar
- B. changing the business objectiv
- C. performing a risk analysi
- D. authorizing a risk acceptanc

Answer: C

Explanation:

Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. It is highly improbable that a business objective could be changed to accommodate a security standard, while risk acceptance* is a process that derives from the risk analysis.

NEW QUESTION 15

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 19

Investments in information security technologies should be based on:

- A. vulnerability assessment
- B. value analysi
- C. business climat
- 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 23

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 28

An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

- A. Security metrics reports

- B. Risk assessment reports
- C. Business impact analysis (BIA)
- D. Return on security investment report

Answer: B

Explanation:

Performing a risk assessment will allow the information security manager to prioritize the remedial measures and provide a means to convey a sense of urgency to management. Metrics reports are normally contained within the methodology of the risk assessment to give it credibility and provide an ongoing tool. The business impact analysis (BIA) covers continuity risks only. Return on security investment cannot be determined until a plan is developed based on the BIA.

NEW QUESTION 32

The PRIMARY objective of a security steering group is to:

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

Answer: B

Explanation:

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

NEW QUESTION 34

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 37

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 42

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

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

Answer: B

Explanation:

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

NEW QUESTION 45

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 46

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

- A. It is easier to promote security awareness
- B. It is easier to manage and control
- 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 50

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 55

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 60

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 61

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 66

Which of the following is the MOST important information to include in an information security standard?

- A. Creation date
- B. Author name
- C. Initial draft approval date
- D. Last review date

Answer: D

Explanation:

The last review date confirms the currency of the standard, affirming that management has reviewed the standard to assure that nothing in the environment has changed that would necessitate an update to the standard. The name of the author as well as the creation and draft dates are not that important.

NEW QUESTION 70

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 74

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

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

Answer: A

Explanation:

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

NEW QUESTION 78

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

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

Answer: C

Explanation:

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the

proper governance. Organizational budget is not a major impact once good governance models are in place, hence governance will help in effective management of the organization's budget.

NEW QUESTION 79

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 81

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 84

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 86

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

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

Answer: C

Explanation:

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

NEW QUESTION 90

Senior management commitment and support for information security can BEST be obtained through presentations that:

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

Answer: D

Explanation:

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

NEW QUESTION 93

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 98

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 99

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 101

How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

- A. Give organization standards preference over local regulations
- B. Follow local regulations only
- C. Make the organization aware of those standards where local regulations causes conflicts
- D. Negotiate a local version of the organization standards

Answer: D

Explanation:

Adherence to local regulations must always be the priority. Not following local regulations can prove detrimental to the group organization. Following local regulations only is incorrect since there needs to be some recognition of organization requirements. Making an organization aware of standards is a sensible step, but is not a total solution. Negotiating a local version of the organization standards is the most effective compromise in this situation.

NEW QUESTION 103

Which of the following would BEST prepare an information security manager for regulatory reviews?

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

Answer: B

Explanation:

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

NEW QUESTION 108

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

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

Answer: D

Explanation:

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

NEW QUESTION 113

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

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

Answer: C

Explanation:

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

NEW QUESTION 116

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 121

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

- A. Examples of genuine incidents at similar organizations
- B. Statement of generally accepted best practices
- C. Associating realistic threats to corporate objectives
- D. Analysis of current technological exposures

Answer: C

Explanation:

Linking realistic threats to key business objectives will direct executive attention to them. All other options are supportive but not of as great a value as choice C when trying to obtain the funds for a new program.

NEW QUESTION 122

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 124

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 129

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

- A. performance measurement
- B. integration
- C. alignment
- D. value delivery

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 134

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

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

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 135

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 136

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

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

Answer: C

Explanation:

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

NEW QUESTION 138

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 140

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 145

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 150

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

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

Answer: B

Explanation:

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

NEW QUESTION 155

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 life
- B. regulatory and legal requirement
- C. business strategy and direction
- D. application systems and media

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 156

What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

- A. Functional requirements are not adequately considered
- B. User training programs may be inadequate
- C. Budgets allocated to business units are not appropriate
- 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 159

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 161

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

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

Answer: C

Explanation:

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

NEW QUESTION 162

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. TC'O 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 167

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 168

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

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

Answer: D

Explanation:

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

NEW QUESTION 171

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 174

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 175

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 177

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

- A. a data processing agreement
- B. a data protection registration
- 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 181

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 program
- C. mapping the IT systems to key business processes
- 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 183

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 187

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 190

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 193

Who in an organization has the responsibility for classifying information?

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

Answer: D

Explanation:

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

NEW QUESTION 196

Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

- A. The information security department has difficulty filling vacancie
- B. The chief information officer (CIO) approves security policy change
- C. The information security oversight committee only meets quarterl
- D. The data center manager has final signoff on all security project

Answer: D

Explanation:

A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good, qualified information security professionals.

NEW QUESTION 201

Senior management commitment and support for information security can BEST be enhanced through:

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

Answer: C

Explanation:

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

NEW QUESTION 202

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 204

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

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

Answer: D

Explanation:

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

NEW QUESTION 209

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 214

An information security manager must understand the relationship between information security and business operations in order to:

- A. support organizational objective
- B. determine likely areas of noncompliance
- C. assess the possible impacts of compromise
- D. understand the threats to the business

Answer: A

Explanation:

Security exists to provide a level of predictability for operations, support for the activities of the organization and to ensure preservation of the organization. Business operations must be the driver for security activities in order to set meaningful objectives, determine and manage the risks to those activities, and provide a basis to measure the effectiveness of and provide guidance to the security program. Regulatory compliance may or may not be an organizational requirement. If compliance is a requirement, some level of compliance must be supported but compliance is only one aspect. It is necessary to understand the business goals in order to assess potential impacts and evaluate threats. These are some of the ways in which security supports organizational objectives, but they are not the only ways.

NEW QUESTION 217

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

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

Answer: B

Explanation:

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

NEW QUESTION 219

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 that are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

NEW QUESTION 222

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

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

Answer: A

Explanation:

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

NEW QUESTION 225

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 226

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 231

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 233

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 235

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 236

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 238

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 239

The value of information assets is BEST determined by:

- A. individual business manager
- B. business systems analyst
- C. information security managemen
- D. industry averages benchmarkin

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 243

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 246

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 249

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 251

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 252

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 253

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

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

Answer: C

Explanation:

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

NEW QUESTION 255

Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

- A. Strategic business plan
- B. Upcoming financial results
- C. Customer personal information
- D. Previous financial results

Answer: D

Explanation:

Previous financial results are public; all of the other choices are private information and should only be accessed by authorized entities.

NEW QUESTION 260

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 263

What does a network vulnerability assessment intend to identify?

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

Answer: D

Explanation:

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

NEW QUESTION 264

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 268

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 threats
- 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 269

A risk management program would be expected to:

- A. remove all inherent risks
- 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 271

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 272

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

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

Answer: C

Explanation:

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

NEW QUESTION 274

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

- A. Nothing, since a risk assessment was completed during development
- B. A vulnerability assessment should be conducted
- C. A new risk assessment should be performed

D. The new vendor's SAS 70 type II report should be reviewed

Answer: C

Explanation:

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

NEW QUESTION 276

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 277

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

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

Answer: C

Explanation:

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

NEW QUESTION 279

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

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

Answer: C

Explanation:

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

NEW QUESTION 284

An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

- A. Key performance indicators (KPIs)
- B. Business impact analysis (BIA)
- C. Gap analysis
- D. Technical vulnerability assessment

Answer: C

Explanation:

Gap analysis would help identify the actual gaps between the desired state and the current implementation of information security management. BIA is primarily used for business continuity planning. Technical vulnerability assessment is used for detailed assessment of technical controls, which would come later in the process and would not provide complete information in order to identify gaps.

NEW QUESTION 288

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 291

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 294

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- A. Control risk
- B. Inherent risk
- C. Risk exposure
- D. Residual risk

Answer: D

Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

NEW QUESTION 297

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 v
- 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 299

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 300

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

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

Answer: C

Explanation:

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

NEW QUESTION 303

A risk analysis should:

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

Answer: C

Explanation:

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

NEW QUESTION 307

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 losse
- B. recommend not renewing the contract upon expiratio
- C. recommend the immediate termination of the contrac
- D. determine the current level of securit

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 311

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 316

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 insuranc
- B. implement a circuit-level firewall to protect the networ
- C. increase the resiliency of security measures in plac
- D. implement a real-time intrusion detection syste

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 317

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

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

Answer: B

Explanation:

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

NEW QUESTION 318

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 323

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 327

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 CIO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

NEW QUESTION 331

The valuation of IT assets should be performed by:

- A. an IT security manager
- B. an independent security consultant

- C. the chief financial officer (CFO).
- D. the information owner

Answer: D

Explanation:

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

NEW QUESTION 335

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

- A. business threats are constantly changing
- B. omissions in earlier assessments can be addressed
- C. repetitive assessments allow various methodologies
- D. they help raise awareness on security in the business

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 336

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 341

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

- A. operations are too busy to comply
- B. the risk is justified by the benefits
- C. policy compliance would be difficult to enforce
- D. users may initially be inconvenienced

Answer: B

Explanation:

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

NEW QUESTION 344

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

- A. Justification of the security budget must be continually made
- B. New vulnerabilities are discovered every day
- C. The risk environment is constantly changing
- D. Management needs to be continually informed about emerging risks

Answer: C

Explanation:

The risk environment is impacted by factors such as changes in technology, and business strategy. These changes introduce new threats and vulnerabilities to the organization. As a result, risk assessment should be performed continuously. Justification of a budget should never be the main reason for performing a risk assessment. New vulnerabilities should be managed through a patch management process. Informing management about emerging risks is important, but is not the main driver for determining when a risk assessment should be performed.

NEW QUESTION 345

A risk management program should reduce risk to:

- A. zero
- B. an acceptable level
- C. an acceptable percent of revenue
- D. an acceptable probability of occurrence

Answer: B

Explanation:

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

NEW QUESTION 346

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

- A. policy development
- B. change management
- C. awareness training
- D. regular monitoring

Answer: B

Explanation:

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

NEW QUESTION 350

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

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

Answer: D

Explanation:

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

NEW QUESTION 352

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

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

Answer: C

Explanation:

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

NEW QUESTION 354

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

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

Answer: B

Explanation:

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or

to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

NEW QUESTION 358

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

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

Answer: B

Explanation:

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

NEW QUESTION 360

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

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

Answer: B

Explanation:

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

NEW QUESTION 364

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 processes
- C. by external parties to maintain objectivity
- D. annually or whenever there is a significant change

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 365

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 367

A risk management approach to information protection is:

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

Answer: A

Explanation:

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

NEW QUESTION 370

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

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

Answer: B

Explanation:

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

NEW QUESTION 373

Who is responsible for ensuring that information is classified?

- A. Senior management
- B. Security manager
- C. Data owner
- D. Custodian

Answer: C

Explanation:

The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

NEW QUESTION 377

An information security organization should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 379

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 381

Information security managers should use risk assessment techniques to:

- A. justify selection of risk mitigation strategie

- B. maximize the return on investment (RO)
- C. provide documentation for auditors and regulator
- D. quantify risks that would otherwise be subjectiv

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 384

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

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

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 387

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 389

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

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

Answer: C

Explanation:

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

NEW QUESTION 392

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

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

Answer: D

Explanation:

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

NEW QUESTION 395

When residual risk is minimized:

- A. acceptable risk is probabl

- B. transferred risk is acceptabl
- C. control risk is reduce
- D. risk is transferabl

Answer: A

Explanation:

Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

NEW QUESTION 400

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

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

Answer: B

Explanation:

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

NEW QUESTION 402

Quantitative risk analysis is MOST appropriate when assessment data:

- A. include customer perception
- B. contain percentage estimate
- C. do not contain specific detail
- D. contain subjective informatio

Answer: B

Explanation:

Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

NEW QUESTION 406

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

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

Answer: B

Explanation:

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

NEW QUESTION 409

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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