

CISM Dumps

Certified Information Security Manager

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



NEW QUESTION 1

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 2

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: A

Explanation:

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

NEW QUESTION 5

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

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

Answer: D

Explanation:

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

NEW QUESTION 6

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 7

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 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

The PRIMARY objective of a security steering group is to:

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

Answer: B

Explanation:

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

NEW QUESTION 10

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 10

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 11

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

- A. aligned with the IT strategic pla
- B. based on the current rate of technological chang
- C. three-to-five years for both hardware and softwar
- D. aligned with the business strateg

Answer: D

Explanation:

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

NEW QUESTION 15

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

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

Answer: D

Explanation:

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

NEW QUESTION 16

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

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

Answer: D

Explanation:

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

NEW QUESTION 21

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 22

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 27

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

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

Answer: B

Explanation:

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

NEW QUESTION 29

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 34

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

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

Answer: A

Explanation:

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

NEW QUESTION 38

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

- A. Procedures for hardening database servers
- B. Standards for password length and complexity
- C. Policies addressing information security governance
- D. Standards for document retention and destruction

Answer: A

Explanation:

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

NEW QUESTION 43

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

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

Answer: A

Explanation:

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

NEW QUESTION 46

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 50

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

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

Answer: A

Explanation:

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

NEW QUESTION 55

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 60

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 65

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 68

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 71

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

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

Answer: A

Explanation:

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

NEW QUESTION 72

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

- A. establishing a periodic risk assessment
- B. promoting regulatory requirement

- C. developing a business cas
- D. developing effective metric

Answer: C

Explanation:

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

NEW QUESTION 73

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 74

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

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

Answer: B

Explanation:

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

NEW QUESTION 75

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 77

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 80

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 82

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

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

Answer: A

Explanation:

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

NEW QUESTION 83

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

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

Answer: D

Explanation:

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

NEW QUESTION 84

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

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

Answer: D

Explanation:

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

NEW QUESTION 87

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 89

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

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

Answer: B

Explanation:

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

NEW QUESTION 91

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 (TC'O)
- 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 95

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 100

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

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

Answer: A

Explanation:

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

NEW QUESTION 101

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

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

Answer:

C

Explanation:

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

NEW QUESTION 103

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

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

Answer: A

Explanation:

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

NEW QUESTION 106

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 109

The MOST important component of a privacy policy is:

- A. notification
- B. warrantie
- C. liabilitie
- D. geographic coverag

Answer: A

Explanation:

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

NEW QUESTION 114

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 118

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

- A. a data processing agreemen

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

Answer: C

Explanation:

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

NEW QUESTION 121

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 124

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 125

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 127

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

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

Answer: C

Explanation:

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

NEW QUESTION 131

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

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

Answer: D

Explanation:

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

NEW QUESTION 134

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

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

Answer: B

Explanation:

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

NEW QUESTION 138

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

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

Answer: C

Explanation:

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

NEW QUESTION 139

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 144

In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

- A. prepare a security budge
- B. conduct a risk assessmen
- C. develop an information security polic
- D. obtain benchmarking informatio

Answer: B

Explanation:

Risk assessment, evaluation and impact analysis will be the starting point for driving management's attention to information security. All other choices will follow the risk assessment.

NEW QUESTION 146

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 150

Acceptable risk is achieved when:

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

Answer: A

Explanation:

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

NEW QUESTION 153

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 158

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 160

The PRIMARY purpose of using risk analysis within a security program is to:

- A. justify the security expenditur
- B. help businesses prioritize the assets to be protecte
- C. inform executive management of residual risk valu
- D. assess exposures and plan remediatio

Answer: D

Explanation:

Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

NEW QUESTION 164

Risk management programs are designed to reduce risk to:

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

Answer: C

Explanation:

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

NEW QUESTION 168

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 171

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 175

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

- A. Implement a security committe
- B. Perform a gap analysi
- C. Implement compensating control
- D. Demand immediate complianc

Answer: B

Explanation:

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

NEW QUESTION 178

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 181

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 184

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 187

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

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

Answer: D

Explanation:

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

NEW QUESTION 189

After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

- A. Information security officer
- B. Chief information officer (CIO)
- C. Business owner
- D. Chief executive officer (CEO)

Answer: C

Explanation:

The business owner of the application needs to understand and accept the residual application risks.

NEW QUESTION 194

What does a network vulnerability assessment intend to identify?

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

Answer: D

Explanation:

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

NEW QUESTION 196

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 197

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

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

Answer: B

Explanation:

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

NEW QUESTION 202

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 207

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

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

Answer: D

Explanation:

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

NEW QUESTION 210

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

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

Answer: B

Explanation:

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

NEW QUESTION 212

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

- A. Nothing, since a risk assessment was completed during developmen
- B. A vulnerability assessment should be conducte
- C. A new risk assessment should be performe
- D. The new vendor's SAS 70 type II report should be reviewe

Answer: C

Explanation:

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

NEW QUESTION 214

A risk mitigation report would include recommendations for:

- A. assessmen
- B. acceptance
- C. evaluatio
- D. quantificatio

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 216

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

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

Answer: C

Explanation:

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

NEW QUESTION 218

Risk assessment is MOST effective when performed:

- A. at the beginning of security program developmen
- B. on a continuous basi
- C. while developing the business case for the security progra
- D. during the business change proces

Answer: B

Explanation:

Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

NEW QUESTION 219

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

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

Answer: A

Explanation:

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

NEW QUESTION 222

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

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

Answer: B

Explanation:

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

NEW QUESTION 226

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

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

Answer: D

Explanation:

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

NEW QUESTION 231

Which of the following 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 236

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

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

Answer: C

Explanation:

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

NEW QUESTION 238

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

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

Answer: D

Explanation:

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

NEW QUESTION 242

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 244

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

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

Answer: A

Explanation:

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

NEW QUESTION 247

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

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

Answer: C

Explanation:

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

NEW QUESTION 250

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 253

The PRIMARY objective of a risk management program is to:

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

Answer: D

Explanation:

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

NEW QUESTION 254

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 departmen
- B. database administrato
- C. chief information officer (CIO).
- D. head of the sales departmen

Answer: D

Explanation:

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

NEW QUESTION 256

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- A. Historical cost of the asset
- B. Acceptable level of potential business impacts
- C. Cost versus benefit of additional mitigating controls
- D. Annualized loss expectancy (ALE)

Answer: C

Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

NEW QUESTION 260

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

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

Answer: A

Explanation:

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

NEW QUESTION 261

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

- A. operations are too busy to compl
- B. the risk is justified by the benefi
- C. policy compliance would be difficult to enforc
- D. users may initially be inconvenience

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 262

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 266

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 271

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

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

Answer: B

Explanation:

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

NEW QUESTION 272

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

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

Answer: A

Explanation:

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

NEW QUESTION 277

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- A. Prevent the system from being accessed remotely
- B. Create a strong random password
- C. Ask for a vendor patch
- D. Track usage of the account by audit trails

Answer: B

Explanation:

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

NEW QUESTION 279

The purpose of a corrective control is to:

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

Answer: C

Explanation:

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

NEW QUESTION 282

A risk management approach to information protection is:

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

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 285

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

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

Answer: A

Explanation:

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

NEW QUESTION 288

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

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

Answer: C

Explanation:

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

NEW QUESTION 292

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 296

What is the BEST technique to determine which security controls to implement with a limited budget?

- A. Risk analysis
- B. Annualized loss expectancy (ALE) calculations
- C. Cost-benefit analysis
- D. Impact analysis

Answer: C

Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

NEW QUESTION 301

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

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

Answer: C

Explanation:

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

NEW QUESTION 302

Which of the following is MOST essential for a risk management program to be effective?

- A. Flexible security budget
- B. Sound risk baseline
- C. New risks detection
- D. Accurate risk reporting

Answer: C

Explanation:

All of these procedures are essential for implementing risk management. However, without identifying new risks, other procedures will only be useful for a limited period.

NEW QUESTION 305

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 309

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 314

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 319

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

- A. Theft of purchased software
- B. Power outage lasting 24 hours
- C. Permanent decline in customer confidence
- D. Temporary loss of e-mail due to a virus attack

Answer: C

Explanation:

A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

NEW QUESTION 323

Identification and prioritization of business risk enables project managers to:

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

Answer: C

Explanation:

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

NEW QUESTION 325

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

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

Answer: B

Explanation:

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

NEW QUESTION 327

Who can BEST advocate the development of and ensure the success of an information security program?

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

Answer: C

Explanation:

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

NEW QUESTION 332

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

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

Answer: D

Explanation:

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

NEW QUESTION 333

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

- A. provide in-depth defenses
- B. separate test and production
- C. permit traffic load balancing
- D. prevent a denial-of-service attack

Answer: C

Explanation:

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

NEW QUESTION 335

Which of the following is MOST important for a successful information security program?

- A. Adequate training on emerging security technologies
- B. Open communication with key process owners
- C. Adequate policies, standards and procedures
- D. Executive management commitment

Answer: D

Explanation:

Sufficient executive management support is the most important factor for the success of an information security program. Open communication, adequate training, and good policies and procedures, while important, are not as important as support from top management; they will not ensure success if senior management support is not present.

NEW QUESTION 339

When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

- A. to a higher false reject rate (FRR).
- B. to a lower crossover error rate
- C. to a higher false acceptance rate (FAR).
- D. exactly to the crossover error rate

Answer: A

Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary to reduce sensitivity and thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts—the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

NEW QUESTION 341

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

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

Answer: C

Explanation:

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

NEW QUESTION 344

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

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

Answer: B

Explanation:

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

NEW QUESTION 347

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

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

Answer: D

Explanation:

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

NEW QUESTION 349

An information security program should be sponsored by:

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

Answer: C

Explanation:

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

NEW QUESTION 353

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

- A. The definition of roles and responsibilities

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

Answer: C

Explanation:

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

NEW QUESTION 356

Who can BEST approve plans to implement an information security governance framework?

- A. Internal auditor
- B. Information security management
- C. Steering committee
- D. Infrastructure management

Answer: C

Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary' to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

NEW QUESTION 359

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- A. Security in storage and transmission of sensitive data
- B. Provider's level of compliance with industry standards
- C. Security technologies in place at the facility
- D. Results of the latest independent security review

Answer: A

Explanation:

How the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

NEW QUESTION 364

Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

- A. Interoffice a system-generated complex password with 30 days expiration
- B. Give a dummy password over the telephone set for immediate expiration
- C. Require no password but force the user to set their own in 10 days
- D. Set initial password equal to the user ID with expiration in 30 days

Answer: B

Explanation:

Documenting the password on paper is not the best method even if sent through interoffice mail if the password is complex and difficult to memorize, the user will likely keep the printed password and this creates a security concern. A dummy (temporary) password that will need to be changed upon first logon is the best method because it is reset immediately and replaced with the user's choice of password, which will make it easier for the user to remember. If it is given to the wrong person, the legitimate user will likely notify security if still unable to access the system, so the security risk is low. Setting an account with no initial password is a security concern even if it is just for a few days. Choice D provides the greatest security threat because user IDs are typically known by both users and security staff, thus compromising access for up to 30 days.

NEW QUESTION 369

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

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

Answer: A

Explanation:

The authentication process is broken because, although the session is valid, the application should reauthenticate when the input parameters are changed. The

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

NEW QUESTION 374

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

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

Answer: B

Explanation:

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

NEW QUESTION 376

A border router should be placed on which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 378

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

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

Answer: C

Explanation:

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

NEW QUESTION 379

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

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

Answer: D

Explanation:

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

NEW QUESTION 381

Which of the following devices should be placed within a demilitarized zone (DMZ)?

- A. Network switch
- B. Web server
- C. Database server
- D. File/print server

Answer: B

Explanation:

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

NEW QUESTION 383

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

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

Answer: A

Explanation:

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

NEW QUESTION 386

Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

- A. Gantt chart
- B. Waterfall chart
- C. Critical path
- D. Rapid Application Development (RAD)

Answer: C

Explanation:

The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

NEW QUESTION 388

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

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

Answer: B

Explanation:

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

NEW QUESTION 392

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

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

Answer: A

Explanation:

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

NEW QUESTION 397

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- A. invite an external consultant to create the security strateg

- B. allocate budget based on best practice
- C. benchmark similar organization
- D. define high-level business security requirement

Answer: D

Explanation:

All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

NEW QUESTION 400

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

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

Answer: B

Explanation:

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

NEW QUESTION 404

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

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

Answer: A

Explanation:

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

NEW QUESTION 409

What is the BEST defense against a Structured Query Language (SQL) injection attack?

- A. Regularly updated signature files
- B. A properly configured firewall
- C. An intrusion detection system
- D. Strict controls on input fields

Answer: D

Explanation:

Structured Query Language (SQL) injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent of fooling the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written; software is available to test for such weaknesses. All other choices would fail to prevent such an attack.

NEW QUESTION 411

The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

- A. helps ensure that communications are secure
- B. increases security between multi-tier system
- C. allows passwords to be changed less frequently
- D. eliminates the need for secondary authentication

Answer: A

Explanation:

Virtual Private Network (VPN) tunneling for remote users provides an encrypted link that helps ensure secure communications. It does not affect password change frequency, nor does it eliminate the need for secondary authentication or affect security within the internal network.

NEW QUESTION 415

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

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

Answer: A

Explanation:

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

NEW QUESTION 418

Which of the following is a key area of the ISO 27001 framework?

- A. Operational risk assessment
- B. Financial crime metrics
- C. Capacity management
- D. Business continuity management

Answer: D

Explanation:

Operational risk assessment, financial crime metrics and capacity management can complement the information security framework, but only business continuity management is a key component.

NEW QUESTION 423

An extranet server should be placed:

- A. outside the firewall
- B. on the firewall server
- C. on a screened subnet
- D. on the external route

Answer: C

Explanation:

An extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

NEW QUESTION 426

Which of the following is the MOST effective type of access control?

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

Answer: B

Explanation:

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

NEW QUESTION 428

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

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

Answer: D

Explanation:

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

NEW QUESTION 429

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

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

Answer: D

Explanation:

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

NEW QUESTION 434

Which of the following devices should be placed within a DMZ?

- A. Router
- B. Firewall
- C. Mail relay
- D. Authentication server

Answer: C

Explanation:

A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ, network segment.

NEW QUESTION 438

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

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

Answer: C

Explanation:

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

NEW QUESTION 439

On which of the following should a firewall be placed?

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

Answer: D

Explanation:

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

NEW QUESTION 440

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

- A. revise the information security progra
- B. evaluate a balanced business scorecar
- C. conduct regular user awareness session
- D. perform penetration test

Answer: B

Explanation:

The balanced business scorecard can track the effectiveness of how an organization executes its information security strategy and determine areas of improvement. Revising the information security program may be a solution, but is not the best solution to improve alignment of the information security objectives. User awareness is just one of the areas the organization must track through the balanced business scorecard. Performing penetration tests does not affect alignment with information security objectives.

NEW QUESTION 445

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

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

Answer: A

Explanation:

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

NEW QUESTION 450

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

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

Answer: B

Explanation:

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

NEW QUESTION 453

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

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

Answer: C

Explanation:

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

NEW QUESTION 457

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- A. a strong authenticatio
- B. IP antispoofing filterin
- C. network encryption protoco
- D. access lists of trusted device

Answer: A

Explanation:

Strong authentication will provide adequate assurance on the identity of the users, while IP antispoofing is aimed at the device rather than the user. Encryption protocol ensures data confidentiality and authenticity while access lists of trusted devices are easily exploited by spoofed identity of the clients.

NEW QUESTION 461

Secure customer use of an e-commerce application can BEST be accomplished through:

- A. data encryptio
- B. digital signature
- C. strong password

D. two-factor authenticatio

Answer: A

Explanation:

Encryption would be the preferred method of ensuring confidentiality in customer communications with an e-commerce application. Strong passwords, by themselves, would not be sufficient since the data could still be intercepted, while two-factor authentication would be impractical. Digital signatures would not provide a secure means of communication. In most business-to-customer (B-to-C) web applications, a digital signature is also not a practical solution.

NEW QUESTION 464

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

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

Answer: C

Explanation:

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

NEW QUESTION 467

.....

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>