

Exam Questions CISM

Certified Information Security Manager

<https://www.2passeasy.com/dumps/CISM/>



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

NEW QUESTION 2

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- A. Regular password audits
- B. Single sign-on system
- C. Security awareness program
- D. Penalties for noncompliance

Answer: C

Explanation:

To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: D

Explanation:

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

NEW QUESTION 5

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 6

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 7

Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

- A. Obtain the support of the board of director
- B. Improve the content of the information security awareness progra
- C. Improve the employees' knowledge of security policie
- D. Implement logical access controls to the information system

Answer: A

Explanation:

It is extremely difficult to implement an information security program without the aid and support of the board of directors. If they do not understand the importance of security to the achievement of the business objectives, other measures will not be sufficient. Options B and (' are measures proposed to ensure the efficiency of the information security program implementation, but are of less significance than obtaining the aid and support of the board of directors. Option D is a measure to secure the enterprise information, but by itself is not a measure to ensure the broader effectiveness of an information security program.

NEW QUESTION 8

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

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

Answer: B

Explanation:

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

NEW QUESTION 9

Investments in information security technologies should be based on:

- A. vulnerability assessment
- B. value analysi
- C. business climat
- D. audit recommendation

Answer: B

Explanation:

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

NEW QUESTION 10

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

- A. Security metrics reports
- B. Risk assessment reports
- C. Business impact analysis (BIA)

D. Return on security investment report

Answer: B

Explanation:

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

NEW QUESTION 10

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

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

Answer: B

Explanation:

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

NEW QUESTION 13

The MOST complete business case for security solutions is one that.

- A. includes appropriate justificatio
- B. explains the current risk profil
- C. details regulatory requirement
- D. identifies incidents and losse

Answer: A

Explanation:

Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

NEW QUESTION 14

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

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

Answer: B

Explanation:

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

NEW QUESTION 16

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 18

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 22

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

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

Answer: D

Explanation:

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

NEW QUESTION 26

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

- A. be aligned with the corporate business strateg
- B. be based on a sound risk management approac
- C. provide adequate regulatory complianc
- 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 31

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 34

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 countr
- B. A security breach notification might get delayed due to the time differenc
- C. Additional network intrusion detection sensors should be installed, resulting in an additional cos
- 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 36

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

- A. When requested
- B. At testing
- C. At programming
- D. At detail requirements

Answer: D

Explanation:

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

NEW QUESTION 40

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 45

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

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

Answer: C

Explanation:

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

NEW QUESTION 48

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

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

Answer: C

Explanation:

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

NEW QUESTION 50

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 51

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

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

Answer: C

Explanation:

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

NEW QUESTION 55

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 56

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

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

Answer: B

Explanation:

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

NEW QUESTION 61

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 66

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 67

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

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

Answer: B

Explanation:

New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support. Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

NEW QUESTION 68

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 72

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

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

Answer: D

Explanation:

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

NEW QUESTION 75

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

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

Answer: C

Explanation:

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

NEW QUESTION 79

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 83

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 84

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 87

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

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

Answer: A

Explanation:

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

NEW QUESTION 90

Who in an organization has the responsibility for classifying information?

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

Answer: D

Explanation:

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

NEW QUESTION 95

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 99

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 104

Who should drive the risk analysis for an organization?

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

Answer: B

Explanation:

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

NEW QUESTION 109

Information security projects should be prioritized on the basis of:

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

Answer: B

Explanation:

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

NEW QUESTION 111

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 113

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 115

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 117

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

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

Answer: B

Explanation:

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

NEW QUESTION 118

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

- A. Evaluate productivity losses
- B. Assess the impact of confidential data disclosure
- C. Calculate the value of the information or asset
- D. Measure the probability of occurrence of each threat

Answer: C

Explanation:

Calculating the value of the information or asset is the first step in a risk analysis process to determine the impact to the organization, which is the ultimate goal. Determining how much productivity could be lost and how much it would cost is a step in the estimation of potential risk process. Knowing the impact if confidential information is disclosed is also a step in the estimation of potential risk. Measuring the probability of occurrence for each threat identified is a step in performing a threat analysis and therefore a partial answer.

NEW QUESTION 119

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 121

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

- A. justify the security expenditure
- 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 125

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 129

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 130

The MOST effective use of a risk register is to:

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

Answer: C

Explanation:

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

NEW QUESTION 131

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

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

Answer: C

Explanation:

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

NEW QUESTION 133

Previously accepted risk should be:

- A. re-assessed periodically since the risk can be escalated to an unacceptable level due to revised condition
- B. accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptabl
- C. avoided next time since risk avoidance provides the best protection to the compan
- D. removed from the risk log once it is accepte

Answer: A

Explanation:

Acceptance of risk should be regularly reviewed to ensure that the rationale for the initial risk acceptance is still valid within the current business context. The rationale for initial risk acceptance may no longer be valid due to change(s) and. hence, risk cannot be accepted permanently. Risk is an inherent part of business and it is impractical and costly to eliminate all risk. Even risks that have been accepted should be monitored for changing conditions that could alter the original decision.

NEW QUESTION 135

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 antispysware policies. Security design flaws require a deeper level of analysis.

NEW QUESTION 138

A risk management program would be expected to:

- A. remove all inherent ris
- B. maintain residual risk at an acceptable leve
- C. implement preventive controls for every threa
- D. reduce control risk to zer

Answer: B

Explanation:

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

NEW QUESTION 141

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

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

Answer: C

Explanation:

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

NEW QUESTION 146

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 149

Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

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

Answer: B

Explanation:

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

NEW QUESTION 153

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

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

Answer: C

Explanation:

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

NEW QUESTION 154

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 159

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 164

Which of the following are the essential ingredients of a business impact analysis (BIA)?

- A. Downtime tolerance, resources and criticality
- B. Cost of business outages in a year as a factor of the security budget
- C. Business continuity testing methodology being deployed

D. Structure of the crisis management team

Answer: A

Explanation:

The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function. Options B, C and D are all associated with business continuity planning, but are not related to the BIA.

NEW QUESTION 169

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

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

Answer: B

Explanation:

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

NEW QUESTION 172

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- A. Business impact analyses
- B. Security gap analyses
- C. System performance metrics
- D. Incident response processes

Answer: B

Explanation:

A security gap analysis is a process which measures all security controls in place against typically good business practice, and identifies related weaknesses. A business impact analysis is less suited to identify security deficiencies. System performance metrics may indicate security weaknesses, but that is not their primary purpose. Incident response processes exist for cases where security weaknesses are exploited.

NEW QUESTION 173

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

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

Answer: D

Explanation:

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

NEW QUESTION 177

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

- A. Implement countermeasure
- B. Eliminate the 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 180

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

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

Answer: B

Explanation:

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

NEW QUESTION 182

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 183

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 188

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 192

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 196

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

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

Answer: C

Explanation:

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

NEW QUESTION 198

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 200

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

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

Answer: B

Explanation:

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

NEW QUESTION 204

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 208

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 211

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 213

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 214

An information security organization should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 216

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

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

Answer: C

Explanation:

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

NEW QUESTION 220

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

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

Answer:

C

Explanation:

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

NEW QUESTION 224

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

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

Answer: C

Explanation:

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

NEW QUESTION 225

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 226

In assessing risk, it is MOST essential to:

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

Answer: C

Explanation:

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

NEW QUESTION 228

Which two components PRIMARILY must be assessed in an effective risk analysis?

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

Answer: B

Explanation:

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

NEW QUESTION 233

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

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

Answer: B

Explanation:

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

NEW QUESTION 237

Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

- A. Baseline security standards
- B. System access violation logs
- C. Role-based access controls
- D. Exit routines

Answer: C

Explanation:

Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Violation logs are detective and do not prevent unauthorized access. Baseline security standards do not prevent unauthorized access. Exit routines are dependent upon appropriate role-based access.

NEW QUESTION 238

An information security manager uses security metrics to measure the:

- A. performance of the information security progra
- B. performance of the security baselin
- C. effectiveness of the security risk analysi
- D. effectiveness of the incident response tea

Answer: A

Explanation:

The security metrics should be designed so that there is a relationship to the performance of the overall security program in terms of effectiveness measurement. Use of security metrics occurs after the risk assessment process and does not measure it. Measurement of the incident response team performance is included in the overall program performance, so this is an incomplete answer.

NEW QUESTION 242

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 247

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 productio
- C. permit traffic load balancin
- D. prevent a denial-of-service attac

Answer: C

Explanation:

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

NEW QUESTION 251

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 255

Which of the following is the BEST metric for evaluating the effectiveness of security awareness training? The number of:

- A. password reset
- B. reported incident
- C. incidents resolved
- D. access rule violation

Answer: B

Explanation:

Reported incidents will provide an indicator of the awareness level of staff. An increase in reported incidents could indicate that the staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. The number of incidents resolved may not correlate to staff awareness.

NEW QUESTION 257

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

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

Answer: C

Explanation:

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

NEW QUESTION 259

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 262

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 265

An information security program should be sponsored by:

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

Answer: C

Explanation:

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

NEW QUESTION 266

Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

- A. Redundant power supplies
- B. Protective switch covers
- C. Shutdown alarms
- D. Biometric readers

Answer: B

Explanation:

Protective switch covers would reduce the possibility of an individual accidentally pressing the power button on a device, thereby turning off the device. Redundant power supplies would not prevent an individual from powering down a device. Shutdown alarms would be after the fact. Biometric readers would be used to control access to the systems.

NEW QUESTION 267

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 271

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 273

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

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

Answer: C

Explanation:

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

NEW QUESTION 274

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:

Now 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 278

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

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

Answer: D

Explanation:

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

NEW QUESTION 283

The MAIN goal of an information security strategic plan is to:

- A. develop a risk assessment pla
- B. develop a data protection pla
- C. protect information assets and resource
- D. establish security governanc

Answer: C

Explanation:

The main goal of an information security strategic plan is to protect information assets and resources. Developing a risk assessment plan and H data protection plan, and establishing security governance refer to tools utilized in the security strategic plan that achieve the protection of information assets and resources.

NEW QUESTION 288

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

- A. Biometric authentication
- B. Embedded steganographic
- C. Two-factor authentication
- D. Embedded digital signature

Answer: D

Explanation:

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

NEW QUESTION 293

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- A. Stress testing
- B. Patch management
- C. Change management
- D. Security baselines

Answer: C

Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves

the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

NEW QUESTION 298

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 299

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

- A. Configuration of firewalls
- B. Strength of encryption algorithms
- C. Authentication within application
- D. Safeguards over keys

Answer: D

Explanation:

If keys are in the wrong hands, documents will be able to be read regardless of where they are on the network. Choice A is incorrect because firewalls can be perfectly configured, but if the keys make it to the other side, they will not prevent the document from being decrypted. Choice B is incorrect because even easy encryption algorithms require adequate resources to break, whereas encryption keys can be easily used. Choice C is incorrect because the application "front door" controls may be bypassed by accessing data directly.

NEW QUESTION 303

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 308

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

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

Answer: B

Explanation:

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

NEW QUESTION 312

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

- A. number of attacks blocke
- B. number of packets droppe
- C. average throughput rat
- D. number of firewall rule

Answer: A

Explanation:

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

NEW QUESTION 313

Which of the following is MOST effective in preventing security weaknesses in operating systems?

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

Answer: A

Explanation:

Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

NEW QUESTION 318

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 319

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

- A. calculating the residual risk
- B. enforcing the security standard
- C. redesigning the system change
- D. implementing mitigating controls

Answer: A

Explanation:

Decisions regarding security should always weigh the potential loss from a risk against the existing controls. Each situation is unique; therefore, it is not advisable to always decide in favor of enforcing a standard. Redesigning the proposed change might not always be the best option because it might not meet the business needs. Implementing additional controls might be an option, but this would be done after the residual risk is known.

NEW QUESTION 323

Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

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

Answer: B

Explanation:

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

NEW QUESTION 327

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 332

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

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

Answer: B

Explanation:

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

NEW QUESTION 336

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 338

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

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

Answer: C

Explanation:

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

NEW QUESTION 340

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 342

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 347

Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

- A. Number of attacks detected
- B. Number of successful attacks
- C. Ratio of false positives to false negatives
- D. Ratio of successful to unsuccessful attacks

Answer: C

Explanation:

The ratio of false positives to false negatives will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while, at the same time, minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

NEW QUESTION 348

What is the MOST important reason for conducting security awareness programs throughout an organization?

- A. Reducing the human risk
- B. Maintaining evidence of training records to ensure compliance
- C. Informing business units about the security strategy
- D. Training personnel in security incident response

Answer: A

Explanation:

People are the weakest link in security implementation, and awareness would reduce this risk. Through security awareness and training programs, individual employees can be informed and sensitized on various security policies and other security topics, thus ensuring compliance from each individual. Laws and regulations also aim to reduce human risk. Informing business units about the security strategy is best done through steering committee meetings or other forums.

NEW QUESTION 352

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

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

Answer: A

Explanation:

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

NEW QUESTION 355

When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

- A. Number of controls
- B. Cost of achieving control objectives
- C. Effectiveness of controls
- D. Test results of controls

Answer: B

Explanation:

Comparison of cost of achievement of control objectives and corresponding value of assets sought to be protected would provide a sound basis for the information security manager to measure value delivery. Number of controls has no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated. Effectiveness of controls has no correlation with the value of assets unless their costs are also evaluated. Test results of controls have no

correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated.

NEW QUESTION 357

The information classification scheme should:

- A. consider possible impact of a security breac
- B. classify personal information in electronic for
- C. be performed by the information security manage
- D. classify systems according to the data processe

Answer: A

Explanation:

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Systems are not classified per se, but the data they process and store should definitely be classified.

NEW QUESTION 359

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

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

Answer: B

Explanation:

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

NEW QUESTION 361

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 363

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

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

Answer: C

Explanation:

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

NEW QUESTION 367

Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

- A. Periodic focus group meetings
- B. Periodic compliance reviews
- C. Computer-based certification training (CBT)
- D. Employee's signed acknowledgement

Answer: C

Explanation:

Using computer-based training (CBT) presentations with end-of-section reviews provides feedback on how well users understand what has been presented. Periodic compliance reviews are a good tool to identify problem areas but do not ensure that procedures are known or understood. Eocus groups may or may not provide meaningful detail. Although a signed employee acknowledgement is good, it does not indicate whether the material has been read and/or understood.

NEW QUESTION 368

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 369

Which of the following is the BEST method to securely transfer a message?

- A. Password-protected removable media
- B. Facsimile transmission in a secured room
- C. Using public key infrastructure (PKI) encryption
- D. Steganography

Answer: C

Explanation:

Using public key infrastructure (PKI) is currently accepted as the most secure method to transmit e-mail messages. PKI assures confidentiality, integrity and nonrepudiation. The other choices are not methods that are as secure as PKI. Steganography involves hiding a message in an image.

NEW QUESTION 372

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

- A. Symmetric cryptography
- B. Public key infrastructure (PKI)
- C. Message hashing
- D. Message authentication code

Answer: B

Explanation:

Public key infrastructure (PKI) combines public key encryption with a trusted third party to publish and revoke digital certificates that contain the public key of the sender. Senders can digitally sign a message with their private key and attach their digital certificate (provided by the trusted third party). These characteristics allow senders to provide authentication, integrity validation and nonrepudiation. Symmetric cryptography provides confidentiality. Mashing can provide integrity and confidentiality. Message authentication codes provide integrity.

NEW QUESTION 374

Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

- A. Intrusion detection system (IDS)
- B. IP address packet filtering
- C. Two-factor authentication
- D. Embedded digital signature

Answer: C

Explanation:

Two-factor authentication provides an additional security mechanism over and above that provided by passwords alone. This is frequently used by mobile users needing to establish connectivity to a corporate network. IP address packet filtering would protect against spoofing an internal address but would not provide strong authentication. An intrusion detection system (IDS) can be used to detect an external attack but would not help in authenticating a user attempting to connect. Digital signatures ensure that transmitted information can be attributed to the named sender.

NEW QUESTION 379

Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

- A. An intrusion prevention system (IPS)
- B. An intrusion detection system (IDS)
- C. A host-based intrusion detection system (HIDS)
- D. A host-based firewall

Answer: A

Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect, but not prevent. IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

NEW QUESTION 381

Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

- A. Virtual private network (VPN)
- B. Firewalls and routers
- C. Biometric authentication
- D. Two-factor authentication

Answer: A

Explanation:

Encryption of data in a virtual private network (VPN) ensures that transmitted information is not readable, even if intercepted. Firewalls and routers protect access to data resources inside the network and do not protect traffic in the public network. Biometric and two-factor authentication, by themselves, would not prevent a message from being intercepted and read.

NEW QUESTION 385

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

- A. Proxy server
- B. Application server
- C. Departmental server
- D. Data warehouse server

Answer: B

Explanation:

An application server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Data warehouse and departmental 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. A proxy server forms the inner boundary of the DMZ but is not placed within it.

NEW QUESTION 390

Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

- A. Never use open source tools
- B. Focus only on production servers
- C. Follow a linear process for attacks
- D. Do not interrupt production processes

Answer: D

Explanation:

The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments since, if compromised, the test environment could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than a linear process.

NEW QUESTION 392

Good information security standards should:

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

Answer: A

Explanation:

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

NEW QUESTION 393

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

- A. references from other organization
- B. past experience of the engagement team

- C. sample deliverabl
- D. methodology used in the assessmen

Answer: D

Explanation:

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

NEW QUESTION 395

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

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

Answer: A

Explanation:

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

NEW QUESTION 396

A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

- A. Prepare an impact assessment repor
- B. Conduct a penetration tes
- C. Obtain approval from senior managemen
- D. Back up the firewall configuration and policy file

Answer: A

Explanation:

An impact assessment report needs to be prepared first by providing the justification for the change, analysis of the changes to be made, the impact if the change does not work as expected, priority of the change and urgency of the change request. Choices B, C and D could be important steps, but the impact assessment report should be performed before the other steps.

NEW QUESTION 401

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

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

Answer: A

Explanation:

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

NEW QUESTION 403

Which of the following areas is MOST susceptible to the introduction of security weaknesses?

- A. Database management
- B. Tape backup management
- C. Configuration management
- D. Incident response management

Answer: C

Explanation:

Configuration management provides the greatest likelihood of security weaknesses through misconfiguration and failure to update operating system (OS) code correctly and on a timely basis.

NEW QUESTION 405

Which of the following would be the MOST significant security risk in a pharmaceutical institution?

- A. Compromised customer information
- B. Unavailability of online transactions
- C. Theft of security tokens
- D. Theft of a Research and Development laptop

Answer: D

Explanation:

The research and development department is usually the most sensitive area of the pharmaceutical organization, Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical: therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

NEW QUESTION 407

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

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

Answer: D

Explanation:

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

NEW QUESTION 409

The return on investment of information security can BEST be evaluated through which of the following?

- A. Support of business objectives
- B. Security metrics
- C. Security deliverables
- D. Process improvement models

Answer: A

Explanation:

One way to determine the return on security investment is to illustrate how information security supports the achievement of business objectives. Security metrics measure improvement and effectiveness within the security practice but do not tie to business objectives. Similarly, listing deliverables and creating process improvement models does not necessarily tie into business objectives.

NEW QUESTION 412

Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

- A. the third party provides a demonstration on a test syste
- B. goals and objectives are clearly define
- C. the technical staff has been briefed on what to expec
- D. special backups of production servers are take

Answer: B

Explanation:

The most important action is to clearly define the goals and objectives of the test. Assuming that adequate backup procedures are in place, special backups should not be necessary. Technical staff should not be briefed nor should there be a demo as this will reduce the spontaneity of the test.

NEW QUESTION 417

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

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

Answer: B

Explanation:

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

NEW QUESTION 422

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

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

Answer: A

Explanation:

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

NEW QUESTION 423

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

- A. all use weak encryption
- B. are decrypted by the firewall
- C. may be quarantined by mail filter
- D. may be corrupted by the receiving mail server

Answer: C

Explanation:

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

NEW QUESTION 427

Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

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

Answer: A

Explanation:

A security policy is a general statement to define management objectives with respect to security. The security strategy addresses higher level issues. Guidelines are optional actions and operational tasks. A security baseline is a set of minimum requirements that is acceptable to an organization.

NEW QUESTION 429

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

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

Answer: D

Explanation:

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

NEW QUESTION 434

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

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

Answer: B

Explanation:

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

is an incomplete (vague) answer from the choices given.

NEW QUESTION 438

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

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

Answer: B

Explanation:

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

NEW QUESTION 441

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

- A. Periodic review of network configuration
- B. Review intrusion detection system (IDS) logs for evidence of attacks
- C. Periodically perform penetration tests
- D. Daily review of server logs for evidence of hacker activity

Answer: C

Explanation:

Due to the complexity of firewall rules and router tables, plus the sheer size of intrusion detection systems (IDSs) and server logs, a physical review will be insufficient. The best approach for confirming the adequacy of these configuration settings is to periodically perform attack and penetration tests.

NEW QUESTION 445

Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

- A. Vulnerability scans
- B. Penetration tests
- C. Code reviews
- D. Security audits

Answer: B

Explanation:

A penetration test is normally the only security assessment that can link vulnerabilities together by exploiting them sequentially. This gives a good measurement and prioritization of risks. Other security assessments such as vulnerability scans, code reviews and security audits can help give an extensive and thorough risk and vulnerability overview, but will not be able to test or demonstrate the final consequence of having several vulnerabilities linked together. Penetration testing can give risk a new perspective and prioritize based on the end result of a sequence of security problems.

NEW QUESTION 446

Which of the following is an inherent weakness of signature-based intrusion detection systems?

- A. A higher number of false positives
- B. New attack methods will be missed
- C. Long duration probing will be missed
- D. Attack profiles can be easily spoofed

Answer: B

Explanation:

Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

NEW QUESTION 447

Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

- A. Delivery path tracing
- B. Reverse lookup translation
- C. Out-of-band channels
- D. Digital signatures

Answer: C

Explanation:

Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting ;in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

NEW QUESTION 450

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

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

Answer: B

Explanation:

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

NEW QUESTION 452

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

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

Answer: C

Explanation:

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

NEW QUESTION 455

Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

- A. The number of false positives increases
- B. The number of false negatives increases
- C. Active probing is missed
- D. Attack profiles are ignored

Answer: A

Explanation:

Failure to tune an intrusion detection system (IDS) will result in many false positives, especially when the threshold is set to a low value. The other options are less likely given the fact that the threshold for sounding an alarm is set to a low value.

NEW QUESTION 456

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

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

Answer: D

Explanation:

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

NEW QUESTION 460

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISM Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISM Product From:

<https://www.2passeasy.com/dumps/CISM/>

Money Back Guarantee

CISM Practice Exam Features:

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