Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
When an organization is implementing an information security governance program, its board of directors should be responsible for:

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

Answer: C

Explanation:

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

NEW QUESTION 2
Which of the following is MOST important to understand when developing a meaningful information security strategy?

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

Answer: D

Explanation:

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

NEW QUESTION 3
It is MOST important that information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

Answer: D

Explanation:

Information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices is secondary by comparison.

NEW QUESTION 4
Which of the following is MOST likely to be discretionary?

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

Answer: C

Explanation:

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

NEW QUESTION 5
From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

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

Answer: D

Explanation:

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

NEW QUESTION 6
An outcome of effective security governance is:

A. business dependency assessment
B. strategic alignmen
C. risk assessmen
D. plannin

Answer: B

Explanation:

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

NEW QUESTION 7
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

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

Answer: D

Explanation:

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

NEW QUESTION 8
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 9
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

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

Answer: A

Explanation:

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

NEW QUESTION 10
Which of the following MOST commonly falls within the scope of an information security governance steering committee?

A. Interviewing candidates for information security specialist positions
B. Developing content for security awareness programs

C. Prioritizing information security initiatives
D. Approving access to critical financial systems

Answer: C

Explanation:

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

NEW QUESTION 10
Who should be responsible for enforcing access rights to application data?

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

Answer: D

Explanation:

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

NEW QUESTION 14
Information security policy enforcement is the responsibility of the:

A. security steering committe
B. chief information officer (CIO).
C. chief information security officer (CISO).
D. chief compliance officer (CCO).

Answer: C

Explanation:

Information security policy enforcement is the responsibility of the chief information security officer (CISO), first and foremost. The board of directors and executive management should ensure that a security policy is in line with corporate objectives. The chief information officer (CIO) and the chief compliance officer (CCO) are involved in the enforcement of the policy but are not directly responsible for it.

NEW QUESTION 17
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 18
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

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

Answer: D

Explanation:

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

NEW QUESTION 19

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

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

Answer: B

Explanation:

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

NEW QUESTION 23
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 25
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Answer: C

Explanation:

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

NEW QUESTION 26
Investment in security technology and processes should be based on:

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

Answer: A

Explanation:

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

NEW QUESTION 29
Which of the following is the MOST important prerequisite for establishing information security management within an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 30
Which of the following is the MOST important information to include in an information security standard?

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

Answer: D

Explanation:

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

NEW QUESTION 32
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

A. Ethics
B. Proportionality
C. Integration
D. Accountability

Answer: B

Explanation:

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules (types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

NEW QUESTION 34
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 39
Minimum standards for securing the technical infrastructure should be defined in a security:

A. strateg
B. guideline
C. mode
D. architectur

Answer: D

Explanation:

Minimum standards for securing the technical infrastructure should be defined in a security architecture document. This document defines how components are secured and the security services that should be in place. A strategy is a broad, high-level document. A guideline is advisory in nature, while a security model shows the relationships between components.

NEW QUESTION 42
Which of the following would BEST prepare an information security manager for regulatory reviews?

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

Answer: B

Explanation:

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

NEW QUESTION 43
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 47
Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

A. baselin
B. strateg
C. procedur
D. polic

Answer: D

Explanation:

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

NEW QUESTION 52
When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

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

Answer: B

Explanation:

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

NEW QUESTION 54
In order to highlight to management the importance of network security, the security manager should FIRST:

A. develop a security architectur
B. install a network intrusion detection system (NIDS) and prepare a list of attack
C. develop a network security polic
D. conduct a risk assessmen

Answer: D

Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

NEW QUESTION 59
Retention of business records should PRIMARILY be based on:

A. business strategy and directio
B. regulatory and legal requirement

C. storage capacity and longevit
D. business ease and value analysi

Answer: B

Explanation:

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

NEW QUESTION 61
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 64
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

A. Compliance with international security standard
B. Use of a two-factor authentication syste
C. Existence of an alternate hot site in case of business disruptio
D. Compliance with the organization's information security requirement

Answer: D

Explanation:

Prom a security standpoint, compliance with the organization's information security requirements is one of the most important topics that should be included in the contract with third-party service provider. The scope of implemented controls in any ISO 27001-compliant organization depends on the security requirements established by each organization. Requiring compliance only with this security standard does not guarantee that a service provider complies with the organization's security requirements. The requirement to use a specific kind of control methodology is not usually stated in the contract with third-party service providers.

NEW QUESTION 69
When designing an information security quarterly report to management, the MOST important element to be considered should be the:

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

Answer: C

Explanation:

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

NEW QUESTION 70
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

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

Answer: B

Explanation:

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

NEW QUESTION 73
Which of the following represents the MAJOR focus of privacy regulations?

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

Answer: D

Explanation:

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

NEW QUESTION 78
Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

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

Answer: C

Explanation:

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

NEW QUESTION 83
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 84
When developing an information security program, what is the MOST useful source of information for determining available resources?

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

Answer: D

Explanation:

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

NEW QUESTION 88
Which of the following roles would represent a conflict of interest for an information security manager?

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

Answer: C

Explanation:

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

NEW QUESTION 90
Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

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

Answer: D

Explanation:

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

NEW QUESTION 95
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 100
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 103
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

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

Answer: B

Explanation:

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

NEW QUESTION 108
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism

C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

Answer: B

Explanation:

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

NEW QUESTION 110
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 112
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 115
Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

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

Answer: D

Explanation:

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

NEW QUESTION 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 123
The PRIMARY purpose of using risk analysis within a security program is to:

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

Answer: D

Explanation:

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

NEW QUESTION 126
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 128
Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

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

Answer: C

Explanation:

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

NEW QUESTION 132
An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

A. threa
B. los
C. vulnerabilit
D. probabilit

Answer: C

Explanation:

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

NEW QUESTION 134
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 139
The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

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

Answer: A

Explanation:

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

NEW QUESTION 140
Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

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

Answer: D

Explanation:

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

NEW QUESTION 141
The security responsibility of data custodians in an organization will include:

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

Answer: D

Explanation:

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

NEW QUESTION 142
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

A. Understand the business requirements of the developer portal
B. Perform a vulnerability assessment of the developer portal
C. Install an intrusion detection system (IDS)
D. Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Answer: A

Explanation:

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

NEW QUESTION 146
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

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

Answer:

B

Explanation:

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

NEW QUESTION 147
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 148
Which of the following roles is PRIMARILY responsible for determining the information
classification levels for a given information asset?

A. Manager
B. Custodian
C. User
D. Owner

Answer: D

Explanation:

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

NEW QUESTION 151
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 154
The recovery time objective (RTO) is reached at which of the following milestones?

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

Answer: C

Explanation:

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

NEW QUESTION 156
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 157
After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

A. transferre
B. treate
C. accepte
D. terminate

Answer: C

Explanation:

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

NEW QUESTION 158
A risk analysis should:

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

Answer: C

Explanation:

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

NEW QUESTION 160
The PRIMARY objective of a risk management program is to:

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

Answer: D

Explanation:

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

NEW QUESTION 161
The valuation of IT assets should be performed by:

A. an IT security manage
B. an independent security consultan
C. the chief financial officer (CFO).
D. the information owne

Answer: D

Explanation:

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

NEW QUESTION 166
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 167
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 169
A risk management program should reduce risk to:

A. zer
B. an acceptable leve
C. an acceptable percent of revenu
D. an acceptable probability of occurrenc

Answer: B

Explanation:

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

NEW QUESTION 173
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

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

Answer: B

Explanation:

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

NEW QUESTION 175
There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

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

Answer: A

Explanation:

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

NEW QUESTION 179
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 180
A risk assessment should be conducted:

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

Answer: D

Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

NEW QUESTION 184
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 185
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 189
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 193
Which of the following is MOST essential for a risk management program to be effective?

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

Answer: C

Explanation:

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

NEW QUESTION 196
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

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

Answer: B

Explanation:

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

NEW QUESTION 198
Which of the following will BEST prevent external security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Securing and analyzing system access logs

Answer: B

Explanation:

Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

NEW QUESTION 200
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

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

Answer: B

Explanation:

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

NEW QUESTION 204
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 208
Which of the following would be the BEST metric for the IT risk management process?

A. Number of risk management action plans
B. Percentage of critical assets with budgeted remedial
C. Percentage of unresolved risk exposures
D. Number of security incidents identified

Answer: B

Explanation:

Percentage of unresolved risk exposures and the number of security incidents identified contribute to the IT risk management process, but the percentage of critical assets with budgeted remedial is the most indicative metric. Number of risk management action plans is not useful for assessing the quality of the process.

NEW QUESTION 213
When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSI.), confidentiality is MOST vulnerable to which of the following?

A. IP spoofing
B. Man-in-the-middle attack
C. Repudiation
D. Trojan

Answer: D

Explanation:

A Trojan is a program that gives the attacker full control over the infected computer, thus allowing the attacker to hijack, copy or alter information after authentication by the user. IP spoofing will not work because IP is not used as an authentication mechanism. Man-in-the-middle attacks are not possible if using SSL with client-side certificates. Repudiation is unlikely because client-side certificates authenticate the user.

NEW QUESTION 215
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. corporate internal audito
B. System developers/analyst
C. key business process owner
D. corporate legal counse

Answer: C

Explanation:

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

NEW QUESTION 218
A test plan to validate the security controls of a new system should be developed during which phase of the project?

A. Testing
B. Initiation
C. Design
D. Development

Answer: C

Explanation:

In the design phase, security checkpoints are defined and a test plan is developed. The testing phase is too late since the system has already been developed and is in production testing. In the initiation phase, the basic security objective of the project is acknowledged. Development is the coding phase and is too late to consider test plans.

NEW QUESTION 220
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 224
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

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

Answer: B

Explanation:

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

NEW QUESTION 228
A digital signature using a public key infrastructure (PKI) will:

A. not ensure the integrity of a messag
B. rely on the extent to which the certificate authority (CA) is truste
C. require two parties to the message exchang
D. provide a high level of confidentialit

Answer: B

Explanation:

The certificate authority (CA) is a trusted third party that attests to the identity of the signatory, and reliance will be a function of the level of trust afforded the CA. A digital signature would provide a level of assurance of message integrity, but it is a three-party exchange, including the CA. Digital signatures do not require encryption of the message in order to preserve confidentiality.

NEW QUESTION 229
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

Answer: A

Explanation:

If an intrusion detection system (IDS) is not properly tuned it will generate an unacceptable number of false positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to operating system hardening, while encryption and packet filtering would not be as relevant.

NEW QUESTION 233
Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

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

Answer: A

Explanation:

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

NEW QUESTION 234
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 236
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 237
The effectiveness of virus detection software is MOST dependent on which of the following?

A. Packet filtering
B. Intrusion detection
C. Software upgrades
D. Definition tables

Answer: D

Explanation:

The effectiveness of virus detection software depends on virus signatures which are stored in virus definition tables. Software upgrades are related to the periodic updating of the program code, which would not be as critical. Intrusion detection and packet filtering do not focus on virus detection.

NEW QUESTION 240
The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

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

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 243
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

A. calculating the residual ris
B. enforcing the security standar
C. redesigning the system chang
D. implementing mitigating control

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 247
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 249
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 l)SB 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 251
An extranet server should be placed:

A. outside the firewal
B. on the firewall serve
C. on a screened subne
D. on the external route

Answer: C

Explanation:

An 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 255
Access control to a sensitive intranet application by mobile users can BEST be implemented through:

A. data encryptio
B. digital signature
C. strong password
D. two-factor authenticatio

Answer: D

Explanation:

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

NEW QUESTION 258
The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

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

Answer: C

Explanation:

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

NEW QUESTION 263
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 265
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 270
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

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

Answer: A

Explanation:

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

NEW QUESTION 275
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 277
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

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

Answer: C

Explanation:

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

NEW QUESTION 279
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 281
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 284
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 organizatio
D. be updated frequently as new software is release

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 289
When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

A. access control matri
B. encryption strengt
C. authentication mechanis
D. data repositor

Answer: A

Explanation:

The access control matrix is the best indicator of the level of compliance with the service level agreement (SLA) data confidentiality clauses. Encryption strength, authentication mechanism and data repository might be defined in the SLA but are not confidentiality compliance indicators.

NEW QUESTION 291
What is the BEST way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards
B. Have the contractors acknowledge in writing the security policies
C. Create penalties for noncompliance in the contracting agreement
D. Perform periodic security reviews of the contractors

Answer: D

Explanation:

Periodic reviews are the most effective way of obtaining compliance. None of the other options detects the failure of contract programmers to comply.

NEW QUESTION 292
Which would be the BEST recommendation to protect against phishing attacks?

A. Install an antispam system
B. Publish security guidance for customers
C. Provide security awareness to the organization's staff
D. Install an application-level firewall

Answer: B

Explanation:

Customers of the organization are the target of phishing attacks. Installing security software or training the organization's staff will be useless. The effort should be put on the customer side.

NEW QUESTION 297
Good information security procedures should:

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

Answer: D

Explanation:

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

NEW QUESTION 298
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

A. The program's governance oversight mechanisms
B. Information security periodicals and manuals
C. The program's security architecture and design
D. Training and certification of the information security team

Answer: A

Explanation:

While choices B, C and D will all assist the currency and coverage of the program, its governance oversight mechanisms are the best method.

NEW QUESTION 299
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 300
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 305
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. polic
B. strateg
C. guideline
D. baselin

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 307
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 311
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 les
B. avoid granting system administration role
C. ensure they successfully pass background check
D. ensure their access is approved by the data owne

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 314
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

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

Answer: C

Explanation:

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

NEW QUESTION 315
Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

A. User ad hoc reporting is not logged
B. Network traffic is through a single switch
C. Operating system (OS) security patches have not been applied
D. Database security defaults to ERP settings

Answer: C

Explanation:

The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security- weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

NEW QUESTION 318
Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 319
Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

A. Provide security awareness training to the third-party provider's employees
B. Conduct regular security reviews of the third-party provider
C. Include security requirements in the service contract
D. Request that the third-party provider comply with the organization's information security policy

Answer: B

Explanation:

Regular security audits and reviews of the practices of the provider to prevent potential information security damage will help verify the security of outsourced services. Depending on the type of services outsourced, security awareness may not be necessary. Security requirements should be included in the contract, but what is most important is verifying that the requirements are met by the provider. It is not necessary to require the provider to fully comply with the policy if only some of the policy is related and applicable.

NEW QUESTION 321
Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

A. Security audit reports
B. Balanced scorecard
C. Capability maturity model (CMM)
D. Systems and business security architecture

Answer: C

Explanation:

The capability maturity model (CMM) grades each defined area of security processes on a scale of 0 to 5 based on their maturity, and is commonly used by entities to measure their existing state and then determine the desired one. Security audit reports offer a limited view of the current state of security. Balanced scorecard is a document that enables management to measure the implementation of their strategy and assists in its translation into action. Systems and business security architecture explain the security architecture of an entity in terms of business strategy, objectives, relationships, risks, constraints and enablers, and provides a business-driven and business-focused view of security architecture.

NEW QUESTION 325
Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Reduced number of security violation reports
B. A quantitative evaluation to ensure user comprehension

C. Increased interest in focus groups on security issues
D. Increased number of security violation reports

Answer: B

Explanation:

To truly judge the effectiveness of security awareness training, some means of measurable testing is necessary to confirm user comprehension. Focus groups may or may not provide meaningful feedback but, in and of themselves, do not provide metrics. An increase or reduction in the number of violation reports may not be indicative of a high level of security awareness.

NEW QUESTION 330
Security policies should be aligned MOST closely with:

A. industry' best practice
B. organizational need
C. generally accepted standard
D. local laws and regulation

Answer: B

Explanation:

The needs of the organization should always take precedence. Best practices and local regulations are important, but they do not take into account the total needs of an organization.

NEW QUESTION 332
What is the BEST way to ensure data protection upon termination of employment?

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

Answer: D

Explanation:

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

NEW QUESTION 336
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

A. Database administrator (DBA)
B. Finance department management
C. Information security manager
D. IT department management

Answer: B

Explanation:

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

NEW QUESTION 338
Which of the following documents would be the BES T reference to determine whether access control mechanisms are appropriate for a critical application?

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

Answer: C

Explanation:

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

NEW QUESTION 342

An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

A. validate and sanitize client side input
B. harden the database listener componen
C. normalize the database schema to the third normal for
D. ensure that the security patches are updated on operating system

Answer: A

Explanation:

SQL injection vulnerability arises when crafted or malformed user inputs are substituted directly in SQL queries, resulting into information leakage. Hardening the database listener does enhance the security of the database; however, it is unrelated to the SQL injection vulnerability. Normalization is related to the effectiveness and efficiency of the database but not to SQL injection vulnerability. SQL injections may also be observed in normalized databases. SQL injection vulnerability exploits the SQL query design, not the operating system.

NEW QUESTION 347
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 349
What is the BEST method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to operating system (OS) patch logs
B. Trace OS patch logs to OS vendor's update documentation
C. Trace OS patch logs to change control requests
D. Review change control documentation for key servers

Answer: C

Explanation:

To ensure that all patches applied went through the change control process, it is necessary to use the operating system (OS) patch logs as a starting point and then check to see if change control documents are on file for each of these changes. Tracing from the documentation to the patch log will not indicate if some patches were applied without being documented. Similarly, reviewing change control documents for key servers or comparing patches applied to those recommended by the OS vendor's web site does not confirm that these security patches were properly approved and documented.

NEW QUESTION 350
The configuration management plan should PRIMARILY be based upon input from:

A. business process owner
B. the information security manage
C. the security steering committe
D. IT senior managemen

Answer: D

Explanation:

Although business process owners, an information security manager and the security steering committee may provide input regarding a configuration management plan, its final approval is the primary responsibility of IT senior management.

NEW QUESTION 351
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
D. Require that a change request be submitted for each download

Answer: A

Explanation:

Administrative accounts have permission to change data. This is not required for the developers to perform their tasks. Unauthorized change will damage the integrity of the data. Logging all usage of the account, suspending the account and activating only when needed, and requiring that a change request be submitted for each download will not reduce the exposure created by this excessive level of access. Restricting the account to read only access will ensure that the integrity can be maintained while permitting access.

NEW QUESTION 356
What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

A. Provide detailed instructions on how to carry out different types of tasks
B. Ensure consistency of activities to provide a more stable environment
C. Ensure compliance to security standards and regulatory requirements
D. Ensure reusability to meet compliance to quality requirements

Answer: B

Explanation:

Developing procedures and guidelines to ensure that business processes address information security risk is critical to the management of an information security program. Developing procedures and guidelines establishes a baseline for security program performance and consistency of security activities.

NEW QUESTION 360
When security policies are strictly enforced, the initial impact is that:

A. they may have to be modified more frequentl
B. they will be less subject to challeng
C. the total cost of security is increase
D. the need for compliance reviews is decrease

Answer: C

Explanation:

When security policies are strictly enforced, more resources are initially required, thereby increasing, the total cost of security. There would be less need for frequent modification. Challenges would be rare and the need for compliance reviews would not necessarily be less.

NEW QUESTION 361
Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

A. Information security officer
B. Security steering committee
C. Data owner
D. Data custodian

Answer: B

Explanation:

Routine administration of all aspects of security is delegated, but senior management must retain overall responsibility. The information security officer supports and implements information security for senior management. The data owner is responsible for categorizing data security requirements. The data custodian supports and implements information security as directed.

NEW QUESTION 365
What is the MOS T cost-effective means of improving security awareness of staff personnel?

A. Employee monetary incentives
B. User education and training
C. A zero-tolerance security policy
D. Reporting of security infractions

Answer: B

Explanation:

User education and training is the most cost-effective means of influencing staff to improve security since personnel are the weakest link in security. Incentives perform poorly without user education and training. A zero-tolerance security policy would not be as good as education and training. Users would not have the knowledge to accurately interpret and report violations without user education and training.

NEW QUESTION 370
Which of the following will BEST protect against malicious activity by a former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

Answer: D

Explanation:

When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important, but are not as effective in preventing this type of situation.

NEW QUESTION 374
The BEST way to ensure that information security policies are followed is to:

A. distribute printed copies to all employee
B. perform periodic reviews for complianc
C. include escalating penalties for noncomplianc
D. establish an anonymous hotline to report policy abuse

Answer: B

Explanation:

The best way to ensure that information security policies are followed is to periodically review levels of compliance. Distributing printed copies, advertising an abuse hotline or linking policies to an international standard will not motivate individuals as much as the consequences of being found in noncompliance. Escalating penalties will first require a compliance review.

NEW QUESTION 376
Which of the following are the MOST important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer
B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal departments

Answer: B

Explanation:

Security steering committees provide a forum for management to express its opinion and take some ownership in the decision making process. It is imperative that business process owners be included in this process. None of the other choices includes input by business process owners.

NEW QUESTION 379
Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

A. Card key door locks
B. Photo identification
C. Awareness training
D. Biometric scanners

Answer: C

Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. Choices A, B and D are physical controls that, by themselves, would not be effective against tailgating.

NEW QUESTION 381
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

A. The right to conduct independent security reviews
B. A legally binding data protection agreement
C. Encryption between the organization and the provider
D. A joint risk assessment of the system

Answer: A

Explanation:

A key requirement of an outsource contract involving critical business systems is the establishment of the organization's right to conduct independent security reviews of the provider's security controls. A legally binding data protection agreement is also critical, but secondary to choice A, which permits examination of the actual security controls prevailing over the system and. as such, is the more effective risk management tool. Network encryption of the link between the organization and the provider may well be a requirement, but is not as critical since it would also be included in choice A. A joint risk assessment of the system in conjunction with the outsource provider may be a compromise solution, should the right to conduct independent security reviews of the controls related to the system prove contractually difficult.

NEW QUESTION 384
In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

A. ensure access to individual functions can be granted to individual users onl
B. implement role-based access control in the applicatio
C. enforce manual procedures ensuring separation of conflicting dutie
D. create service accounts that can only be used by authorized team member

Answer: B

Explanation:

Role-based access control is the best way to implement appropriate segregation of duties. Roles will have to be defined once and then the user could be changed from one role to another without redefining the content of the role each time. Access to individual functions will not ensure appropriate segregation of duties. Giving a user access to all functions and implementing, in parallel, a manual procedure ensuring segregation of duties is not an effective method, and would be difficult to enforce and monitor. Creating service accounts that can be used by authorized team members would not provide any help unless their roles are properly segregated.

NEW QUESTION 387
Which of the following is the BEST approach for an organization desiring to protect its
intellectual property?

A. Conduct awareness sessions on intellectual property policy
B. Require all employees to sign a nondisclosure agreement
C. Promptly remove all access when an employee leaves the organization
D. Restrict access to a need-to-know basis

Answer: D

Explanation:

Security awareness regarding intellectual property policy will not prevent violations of this policy. Requiring all employees to sign a nondisclosure agreement and promptly removing all access when an employee leaves the organization are good controls, but not as effective as restricting access to a need-to- know basis.

NEW QUESTION 392
Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

A. Signal strength
B. Number of administrators
C. Bandwidth
D. Encryption strength

Answer: B

Explanation:

The number of individuals with access to the network configuration presents a security risk. Encryption strength is an area where wireless networks tend to fall short; however, the potential to compromise the entire network is higher when an inappropriate number of people can alter the configuration. Signal strength and network bandwidth are secondary issues.

NEW QUESTION 397
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audit
B. Perform periodic penetration testin
C. Define and monitor security metric
D. Survey business units for feedbac

Answer: C

Explanation:

Defining and monitoring security metrics is a good approach to analyze the performance of the security management process since it determines the baseline and evaluates the performance against the baseline to identify an opportunity for improvement. This is a systematic and structured approach to process improvement. Audits will identify deficiencies in established controls; however, they are not effective in evaluating the overall performance for improvement. Penetration testing will only uncover technical vulnerabilities, and cannot provide a holistic picture of information security management, feedback is subjective and not necessarily reflective of true performance.

NEW QUESTION 398
An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

A. Request that the third-party provider perform background checks on their employee
B. Perform an internal risk assessment to determine needed control
C. Audit the third-party provider to evaluate their security control
D. Perform a security assessment to detect security vulnerabilitie

Answer: B

Explanation:

An internal risk assessment should be performed to identify the risk and determine needed controls. A background check should be a standard requirement for the service provider. Audit objectives should be determined from the risk assessment results. Security assessment does not cover the operational risks.

NEW QUESTION 399

An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

A. source routin
B. broadcast propagatio
C. unregistered port
D. nonstandard protocol

Answer: A

Explanation:

If the firewall allows source routing, any outsider can carry out spoofing attacks by stealing the internal (private) IP addresses of the organization. Broadcast propagation, unregistered ports and nonstandard protocols do not create a significant security exposure.

NEW QUESTION 401
Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System analyst
B. Quality control manager
C. Process owner
D. Information security manager

Answer: C

Explanation:

Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

NEW QUESTION 406
In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

A. volume of sensitive dat
B. recovery point objective (RPO).
C. recovery' time objective (RTO).
D. interruption windo

Answer: B

Explanation:

The recovery point objective (RPO) defines the maximum loss of data (in terms of time) acceptable by the business (i.e., age of data to be restored). It will directly determine the basic elements of the backup strategy frequency of the backups and what kind of backup is the most appropriate (disk-to-disk, on tape, mirroring). The volume of data will be used to determine the capacity of the backup solution. The recovery time objective (RTO)—the time between disaster and return to normal operation—will not have any impact on the backup strategy. The availability to restore backups in a time frame consistent with the interruption window will have to be checked and will influence the strategy (e.g., full backup vs. incremental), but this will not be the primary factor.

NEW QUESTION 409
When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

A. Business continuity plan
B. Disaster recovery plan
C. Incident response plan
D. Vulnerability management plan

Answer: C

Explanation:

An incident response plan documents the step-by-step process to follow, as well as the related roles and responsibilities pertaining to all parties involved in responding to an information security breach. A business continuity plan or disaster recovery plan would be triggered during the execution of the incident response plan in the case of a breach impacting the business continuity. A vulnerability management plan is a procedure to address technical vulnerabilities and mitigate the risk through configuration changes (patch management).

NEW QUESTION 413
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewall
B. bastion host
C. decoy file
D. screened subnet

Answer: C

Explanation:

Decoy files, often referred to as honcypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence.

Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

NEW QUESTION 414
Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

A. Detailed technical recovery plans are maintained offsite
B. Network redundancy is maintained through separate providers
C. Hot site equipment needs are recertified on a regular basis
D. Appropriate declaration criteria have been established

Answer: A

Explanation:

In a major disaster, staff can be injured or can be prevented from traveling to the hot site, so technical skills and business knowledge can be lost. It is therefore critical to maintain an updated copy of the detailed recovery plan at an offsite location. Continuity of the business requires adequate network redundancy, hot site infrastructure that is certified as compatible and clear criteria for declaring a disaster. Ideally, the business continuity program addresses all of these satisfactorily. However, in a disaster situation, where all these elements are present, but without the detailed technical plan, business recovery will be seriously impaired.

NEW QUESTION 415
An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

A. require the use of strong password
B. assign static IP addresse
C. implement centralized logging softwar
D. install an intrusion detection system (IDS).

Answer: D

Explanation:

Installing an intrusion detection system (IDS) will allow the information security manager to better pinpoint the source of the attack so that countermeasures may then be taken. An IDS is not limited to detection of attacks originating externally. Proper placement of agents on the internal network can be effectively used to detect an internally based attack. Requiring the use of strong passwords will not be sufficiently effective against a network-based attack. Assigning IP addresses would not be effective since these can be spoofed. Implementing centralized logging software will not necessarily provide information on the source of the attack.

NEW QUESTION 418
Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

A. Communicating specially drafted messages by an authorized person
B. Refusing to comment until recovery
C. Referring the media to the authorities
D. Reporting the losses and recovery strategy to the media

Answer: A

Explanation:

Proper messages need to be sent quickly through a specific identified person so that there are no rumors or statements made that may damage reputation. Choices B, C and D are not recommended until the message to be communicated is made clear and the spokesperson has already spoken to the media.

NEW QUESTION 423
......

Relate Links

100% Pass Your CISM Exam with Exambible Prep Materials

https://www.exambible.com/CISM-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/