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 would be MOST effective in successfully implementing restrictive password policies?

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

Answer: C

Explanation:

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

NEW QUESTION 3
What would be the MOST significant security risks when using wireless local area network (LAN) technology?

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

Answer: C

Explanation:

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

NEW QUESTION 4
Which of the following would BEST ensure the success of information security governance within an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 5
Which of the following is MOST likely to be discretionary?

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

Answer: C

Explanation:

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

NEW QUESTION 6
An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees Hood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

A. conflicting security controls with organizational need
B. strong protection of information resource
C. implementing appropriate controls to reduce ris
D. proving information security's protective abilitie

Answer: A

Explanation:

The needs of the organization were not taken into account, so there is a conflict. This example is not strong protection, it is poorly configured. Implementing appropriate controls to reduce risk is not an appropriate control as it is being used. This does not prove the ability to protect, but proves the ability to interfere with business.

NEW QUESTION 7
A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

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

Answer: C

Explanation:

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

NEW QUESTION 8
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 9
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 10
Which of the following would help to change an organization's security culture?

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

Answer: B

Explanation:

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

NEW QUESTION 10
Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

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

Answer: A

Explanation:

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

NEW QUESTION 13
Which of the following is the MOST important information to include in a strategic plan for information security?

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

Answer: B

Explanation:

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

NEW QUESTION 14
The PRIMARY goal in developing an information security strategy is to:

A. establish security metrics and performance monitorin
B. educate business process owners regarding their dutie
C. ensure that legal and regulatory requirements are met
D. support the business objectives of the organizatio

Answer: D

Explanation:

The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

NEW QUESTION 15
Effective IT governance is BEST ensured by:

A. utilizing a bottom-up approac
B. management by the IT departmen
C. referring the matter to the organization's legal departmen
D. utilizing a top-down approac

Answer: D

Explanation:

Effective IT governance needs to be a top-down initiative, with the board and executive management setting clear policies, goals and objectives and providing for ongoing monitoring of the same. Focus on the regulatory issues and management priorities may not be reflected effectively by a bottom-up approach. IT governance affects the entire organization and is not a matter concerning only the management of IT. The legal department is part of the overall governance process, but cannot take full responsibility.

NEW QUESTION 17
The MOST basic requirement for an information security governance program is to:

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

D. provide best practices for security- initiative

Answer: A

Explanation:

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

NEW QUESTION 19
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 22
The MOST important characteristic of good security policies is that they:

A. state expectations of IT managemen
B. state only one general security mandat
C. are aligned with organizational goal
D. govern the creation of procedures and guideline

Answer: C

Explanation:

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

NEW QUESTION 23
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

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

Answer: A

Explanation:

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

NEW QUESTION 28
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 30
Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

A. Update platform-level security settings
B. Conduct disaster recovery test exercises
C. Approve access to critical financial systems
D. Develop an information security strategy paper

Answer: D

Explanation:

Developing a strategy paper on information security would be the most appropriate. Approving access would be the job of the data owner. Updating platform-level security and conducting recovery test exercises would be less essential since these are administrative tasks.

NEW QUESTION 33
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 34
To achieve effective strategic alignment of security initiatives, it is important that:

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

Answer: B

Explanation:

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

NEW QUESTION 35
Which of the following is the BEST reason to perform a business impact analysis (BIA)?

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

Answer: A

Explanation:

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

NEW QUESTION 38
Which of the following is the BEST justification to convince management to invest in an information security program?

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

Answer: D

Explanation:

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

NEW QUESTION 43
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 48
When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

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

Answer: B

Explanation:

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

NEW QUESTION 52
Information security should be:

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

Answer: B

Explanation:

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

NEW QUESTION 56
Which of the following would be the MOST important goal of an information security governance program?

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

Answer: D

Explanation:

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

NEW QUESTION 59
The MOST useful way to describe the objectives in the information security strategy is through:

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

Answer: A

Explanation:

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

NEW QUESTION 64
Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

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

Answer: C

Explanation:

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

NEW QUESTION 69
Which of the following characteristics is MOST important when looking at prospective candidates for the role of chief information security officer (CISO)?

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

Answer: B

Explanation:

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

NEW QUESTION 73
An information security manager must understand the relationship between information security and business operations in order to:

A. support organizational objective
B. determine likely areas of noncomplianc
C. assess the possible impacts of compromis
D. understand the threats to the busines

Answer: A

Explanation:

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

NEW QUESTION 76
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 81
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 85
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 90
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

A. map the major threats to business objective
B. review available sources of risk informatio
C. identify the value of the critical asset
D. determine the financial impact if threats materializ

Answer: A

Explanation:

Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

NEW QUESTION 91
The value of information assets is BEST determined by:

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

Answer: A

Explanation:

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

NEW QUESTION 93
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 96
Phishing is BEST mitigated by which of the following?

A. Security monitoring software
B. Encryption
C. Two-factor authentication
D. User awareness

Answer: D

Explanation:

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.

NEW QUESTION 97
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 100
Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. Evaluation
D. Monitoring

Answer: B

Explanation:

Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

NEW QUESTION 105
A successful risk management program should lead to:

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

Answer: A

Explanation:

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

NEW QUESTION 110
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 112
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 114
In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

A. original cost to acquir
B. cost of the software store
C. annualized loss expectancy (ALE).
D. cost to obtain a replacemen

Answer: D

Explanation:

The value of the server should be based on its cost of replacement. The original cost may be significantly different from the current cost and, therefore, not as relevant. The value of the software is not at issue because it can be restored from backup media. The ALE for all risks related to the server does not represent the server's value.

NEW QUESTION 119
A risk mitigation report would include recommendations for:

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

Answer: B

Explanation:

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

NEW QUESTION 123
An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

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

Answer: C

Explanation:

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

NEW QUESTION 128
A common concern with poorly written web applications is that they can allow an attacker to:

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

Answer: D

Explanation:

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

NEW QUESTION 133
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 136
Which of the following attacks is BEST mitigated by utilizing strong passwords?

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

Answer: B

Explanation:

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

NEW QUESTION 140
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

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

Answer: C

Explanation:

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

NEW QUESTION 142
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 145
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 146
Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

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

Answer: D

Explanation:

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

NEW QUESTION 147
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 152
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

A. increase its customer awareness efforts in those region
B. implement monitoring techniques to detect and react to potential frau
C. outsource credit card processing to a third part
D. make the customer liable for losses if they fail to follow the bank's advic

Answer: B

Explanation:

While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk. Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

NEW QUESTION 153
A risk management approach to information protection is:

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

Answer: A

Explanation:

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

NEW QUESTION 157
Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

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

Answer: C

Explanation:

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

NEW QUESTION 158
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 162
An information security organization should PRIMARILY:

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

Answer: A

Explanation:

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

NEW QUESTION 165
What is the BEST technique to determine which security controls to implement with a limited budget?

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

Answer: C

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

NEW QUESTION 170
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 172
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

A. Theft of purchased software

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

Answer: C

Explanation:

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

NEW QUESTION 174
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results
D. Amount of IT budget available

Answer: A

Explanation:

Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

NEW QUESTION 176
An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

A. eliminating the ris
B. transferring the ris
C. mitigating the ris
D. accepting the ris

Answer: C

Explanation:

Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

NEW QUESTION 180
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

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

Answer: C

Explanation:

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

NEW QUESTION 183
An information security manager uses security metrics to measure the:

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

Answer: A

Explanation:

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

NEW QUESTION 188
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 190
Which of the following is MOST important for a successful information security program?

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

Answer: D

Explanation:

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

NEW QUESTION 191
When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 193
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 198
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 201
At what stage of the applications development process would encryption key management initially be addressed?

A. Requirements development
B. Deployment
C. Systems testing
D. Code reviews

Answer: A

Explanation:

Encryption key management has to be integrated into the requirements of the application's design. During systems testing and deployment would be too late since the requirements have already been agreed upon. Code reviews are part of the final quality assurance (QA) process and would also be too late in the process.

NEW QUESTION 205
Which of the following devices should be placed within a demilitarized zone (DMZ)?

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

Answer: B

Explanation:

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

NEW QUESTION 207
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

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

Answer: D

Explanation:

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

NEW QUESTION 211
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 215
Which of the following is a key area of the ISO 27001 framework?

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

Answer: D

Explanation:

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

NEW QUESTION 220
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

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

Answer: C

Explanation:

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

NEW QUESTION 223
Which of the following is the MOST effective type of access control?

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

Answer: B

Explanation:

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

NEW QUESTION 224
Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

A. Regular review of access control lists
B. Security guard escort of visitors
C. Visitor registry log at the door
D. A biometric coupled with a PIN

Answer: A

Explanation:

A review of access control lists is a detective control that will enable an information security manager to ensure that authorized persons are entering in compliance with corporate policy. Visitors accompanied by a guard will also provide assurance but may not be cost effective. A visitor registry is the next cost-effective control. A biometric coupled with a PIN will strengthen the access control; however, compliance assurance logs will still have to be reviewed.

NEW QUESTION 228
On which of the following should a firewall be placed?

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

Answer: D

Explanation:

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

NEW QUESTION 231
What is the MOST important reason for conducting security awareness programs throughout an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 233
It is important to develop an information security baseline because it helps to define:

A. critical information resources needing protectio
B. a security policy for the entire organizatio
C. the minimum acceptable security to be implemente
D. required physical and logical access control

Answer: C

Explanation:

Developing an information security baseline helps to define the minimum acceptable security that will be implemented to protect the information resources in accordance with the respective criticality levels. Before determining the security baseline, an information security manager must establish the security policy, identify criticality levels of organization's information resources and assess the risk environment in which those resources operate.

NEW QUESTION 238
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

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

Answer: B

Explanation:

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

NEW QUESTION 241
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 245
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

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

Answer: B

Explanation:

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

NEW QUESTION 248
Which of the following is the BEST method to securely transfer a message?

A. Password-protected removable media

B. Facsimile transmission in a secured room
C. Using public key infrastructure (PKI) encryption
D. Steganography

Answer: C

Explanation:

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

NEW QUESTION 249
Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

A. Filter media access control (MAC) addresses
B. Use a Wi-Fi Protected Access (WPA2) protocol
C. Use a Wired Equivalent Privacy (WEP) key
D. Web-based authentication

Answer: B

Explanation:

WPA2 is currently one of the most secure authentication and encryption protocols for mainstream wireless products. MAC address filtering by itself is not a good security mechanism since allowed MAC addresses can be easily sniffed and then spoofed to get into the network. WEP is no longer a secure encryption mechanism for wireless communications. The WEP key can be easily broken within minutes using widely available software. And once the WEP key is obtained, all communications of every other wireless client are exposed. Finally, a web-based authentication mechanism can be used to prevent unauthorized user access to a network, but it will not solve the wireless network's main security issues, such as preventing network sniffing.

NEW QUESTION 250
Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

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

Answer: C

Explanation:

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

NEW QUESTION 251
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. messages displayed at every logo
B. periodic security-related e-mail message
C. an Intranet web site for information securit
D. circulating the information security polic

Answer: A

Explanation:

Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet web site does not force users to access it and read the information. Circulating the information security policy atone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

NEW QUESTION 253
Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

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

Answer: A

Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect,

but not prevent I IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

NEW QUESTION 258
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

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

Answer: A

Explanation:

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

NEW QUESTION 262
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

A. Encryption
B. Digital certificate
C. Digital signature
D. I lashing algorithm

Answer: A

Explanation:

To preserve confidentiality of a message while in transit, encryption should be implemented. Choices B and C only help authenticate the sender and the receiver. Choice D ensures integrity.

NEW QUESTION 263
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 265
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 270
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

A. System monitoring for traffic on network ports
B. Security code reviews for the entire application
C. Reverse engineering the application binaries
D. Running the application from a high-privileged account on a test system

Answer: B

Explanation:

Security' code reviews for the entire application is the best measure and will involve reviewing the entire source code to detect all instances of back doors. System monitoring for traffic on network ports would not be able to detect all instances of back doors and is time consuming and would take a lot of effort. Reverse engineering the application binaries may not provide any definite clues. Back doors will not surface by running the application on high-privileged accounts since back doors are usually hidden accounts in the applications.

NEW QUESTION 271
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

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

Answer: B

Explanation:

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

NEW QUESTION 273
In business-critical applications, user access should be approved by the:

A. information security manage
B. data owne
C. data custodia
D. business managemen

Answer: B

Explanation:

A data owner is in the best position to validate access rights to users due to their deep understanding of business requirements and of functional implementation within the application. This responsibility should be enforced by the policy. An information security manager will coordinate and execute the implementation of the role-based access control. A data custodian will ensure that proper safeguards are in place to protect the data from unauthorized access; it is not the data custodian's responsibility to assign access rights. Business management is not. in all cases, the owner of the data.

NEW QUESTION 275
Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to- date can be BEST achieved through which of the following?

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

Answer: D

Explanation:

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

NEW QUESTION 278
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 283
Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

A. Vulnerability scans
B. Penetration tests

C. Code reviews
D. Security audits

Answer: B

Explanation:

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

NEW QUESTION 287
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 289
A critical component of a continuous improvement program for information security is:

A. measuring processes and providing feedbac
B. developing a service level agreement (SLA) for securit
C. tying corporate security standards to a recognized international standar
D. ensuring regulatory complianc

Answer: A

Explanation:

If an organization is unable to take measurements that will improve the level of its safety program. then continuous improvement is not possible. Although desirable, developing a service level agreement (SLA) for security, tying corporate security standards to a recognized international standard and ensuring regulatory compliance are not critical components for a continuous improvement program.

NEW QUESTION 294
The PRIMARY focus of the change control process is to ensure that changes are:

A. authorize
B. applie
C. documente
D. teste

Answer: A

Explanation:

All steps in the change control process must be signed off on to ensure proper authorization. It is important that changes are applied, documented and tested; however, they are not the primary focus.

NEW QUESTION 296
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 297
A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

A. it simulates the real-1ife situation of an external security attac

B. human intervention is not required for this type of tes
C. less time is spent on reconnaissance and information gatherin
D. critical infrastructure information is not revealed to the teste

Answer: C

Explanation:

Data and information required for penetration are shared with the testers, thus eliminating time that would otherwise have been spent on reconnaissance and gathering of information. Blind (black box) penetration testing is closer to real life than full disclosure (white box) testing. There is no evidence to support that human intervention is not required for this type of test. A full disclosure (white box) methodology requires the knowledge of the subject being tested.

NEW QUESTION 298
An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

A. Rule-based
B. Mandatory
C. Discretionary
D. Role-based

Answer: D

Explanation:

Role-based access control is effective and efficient in large user communities because it controls system access by the roles defined for groups of users. Users are assigned to the various roles and the system controls the access based on those roles. Rule-based access control needs to define the access rules, which is troublesome and error prone in large organizations. In mandatory access control, the individual's access to information resources needs to be defined, which is troublesome in large organizations. In discretionary access control, users have access to resources based on predefined sets of principles, which is an inherently insecure approach.

NEW QUESTION 299
The implementation of continuous monitoring controls is the BEST option where:

A. incidents may have a high impact and frequency
B. legislation requires strong information security controls
C. incidents may have a high impact but low frequency
D. Electronic commerce is a primary business driver

Answer: A

Explanation:

Continuous monitoring control initiatives are expensive, so they have to be used in areas where the risk is at its greatest level. These areas are the ones with high impact and high frequency of occurrence. Regulations and legislations that require tight IT security measures focus on requiring organizations to establish an IT security governance structure that manages IT security with a risk-based approach, so each organization decides which kinds of controls are implemented. Continuous monitoring is not necessarily a requirement. Measures such as contingency planning are commonly used when incidents rarely happen but have a high impact each time they happen. Continuous monitoring is unlikely to be necessary. Continuous control monitoring initiatives are not needed in all electronic commerce environments. There are some electronic commerce environments where the impact of incidents is not high enough to support the implementation of this kind of initiative.

NEW QUESTION 303
Managing the life cycle of a digital certificate is a role of a(n):

A. system administrato
B. security administrato
C. system develope
D. independent trusted sourc

Answer: D

Explanation:

Digital certificates must be managed by an independent trusted source in order to maintain trust in their authenticity. The other options are not necessarily entrusted with this capability.

NEW QUESTION 308
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

A. uses multiple redirects for completing a data commit transactio
B. has implemented cookies as the sole authentication mechanis
C. has been installed with a non-1egitimate license ke
D. is hosted on a server along with other application

Answer: B

Explanation:

XSRF exploits inadequate authentication mechanisms in web applications that rely only on elements such as cookies when performing a transaction. XSRF is related to an authentication mechanism, not to redirection. Option C is related to intellectual property rights, not to XSRF vulnerability. Merely hosting multiple applications on the same server is not the root cause of this vulnerability.

NEW QUESTION 309
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 313
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

A. Adequate security policies and procedures
B. Periodic compliance reviews
C. Security steering committees
D. Security awareness campaigns

Answer: D

Explanation:

Security awareness campaigns will be more effective at changing an organizational culture than the creation of steering committees and security policies and procedures. Compliance reviews are helpful; however, awareness by all staff is more effective because compliance reviews are focused on certain areas groups and do not necessarily educate.

NEW QUESTION 318
When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

A. submit the issue to the steering committe
B. conduct an impact analysis to quantify the risk
C. isolate the system from the rest of the networ
D. request a risk acceptance from senior managemen

Answer: B

Explanation:

An impact analysis is warranted to determine whether a risk acceptance should be granted and to demonstrate to the department the danger of deviating from the established policy. Isolating the system would not support the needs of the business. Any waiver should be granted only after performing an impact analysis.

NEW QUESTION 322
Which of the following represents a PRIMARY area of interest when conducting a penetration test?

A. Data mining
B. Network mapping
C. Intrusion Detection System (IDS)
D. Customer data

Answer: B

Explanation:

Network mapping is the process of determining the topology of the network one wishes to penetrate. This is one of the first steps toward determining points of attack in a network. Data mining is associated with ad hoc reporting and. together with customer data, they are potential targets after the network is penetrated. The intrusion detection mechanism in place is not an area of focus because one of the objectives is to determine how effectively it protects the network or how easy it is to circumvent.

NEW QUESTION 323
The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

A. Data owner
B. Data custodian
C. Systems programmer

D. Security administrator

Answer: C

Explanation:

A systems programmer should not have privileges to modify the access control list (ACL) because this would give the programmer unlimited control over the system. The data owner would request and approve updates to the ACL, but it is not a violation of the separation of duties principle if the data owner has update rights to the ACL. The data custodian and the security administrator could carry out the updates on the ACL since it is part of their duties as delegated to them by the data owner.

NEW QUESTION 324
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testin
B. establish security baseline
C. implement vendor default setting
D. link policies to an independent standar

Answer: B

Explanation:

Security baselines will provide the best assurance that each platform meets minimum criteria. Penetration testing will not be as effective and can only be performed periodically. Vendor default settings will not necessarily meet the criteria set by the security policies, while linking policies to an independent standard will not provide assurance that the platforms meet these levels of security.

NEW QUESTION 329
The PRIMARY reason for using metrics to evaluate information security is to:

A. identify security weaknesse
B. justify budgetary expenditure
C. enable steady improvemen
D. raise awareness on security issue

Answer: C

Explanation:

The purpose of a metric is to facilitate and track continuous improvement. It will not permit the identification of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

NEW QUESTION 333
A security awareness program should:

A. present top management's perspectiv
B. address details on specific exploit
C. address specific groups and role
D. promote security department procedure

Answer: C

Explanation:

Different groups of employees have different levels of technical understanding and need awareness training that is customized to their needs; it should not be presented from a specific perspective. Specific details on technical exploits should be avoided since this may provide individuals with knowledge they might misuse or it may confuse the audience. This is also not the best forum in which to present security department procedures.

NEW QUESTION 335
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 336
When an emergency security patch is received via electronic mail, the patch should FIRST be:

A. loaded onto an isolated test machin

B. decompiled to check for malicious cod
C. validated to ensure its authenticit
D. copied onto write-once media to prevent tamperin

Answer: C

Explanation:

It is important to first validate that the patch is authentic. Only then should it be copied onto write-once media, decompiled to check for malicious code or loaded onto an isolated test machine.

NEW QUESTION 340
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 345
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 347
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 351
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 356
Which of the following is generally considered a fundamental component of an information security program?

A. Role-based access control systems
B. Automated access provisioning
C. Security awareness training
D. Intrusion prevention systems (IPSs)

Answer: C

Explanation:

Without security awareness training, many components of the security program may not be effectively implemented. The other options may or may not be necessary, but are discretionary.

NEW QUESTION 357
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

A. Design a training program for the staff involved to heighten information security awareness
B. Set role-based access permissions on the shared folder
C. The end user develops a PC macro program to compare sender and recipient file contents
D. Shared folder operators sign an agreement to pledge not to commit fraudulent activities

Answer: B

Explanation:

Ideally, requesting that the IT department develop an automated integrity check would be desirable, but given the temporary nature of the problem, the risk can be mitigated by setting stringent access permissions on the shared folder. Operations staff should only have write access and disbursement staff should only have read access, and everyone else, including the administrator, should be disallowed. An information security awareness program and/or signing an agreement to not engage in fraudulent activities may help deter attempts made by employees: however, as long as employees see a chance of personal gain when internal control is loose, they may embark on unlawful activities such as alteration of payment files. A PC macro would be an inexpensive automated solution to develop with control reports. However, sound independence or segregation of duties cannot be expected in the reconciliation process since it is run by an end-user group. Therefore, this option may not provide sufficient proof.

NEW QUESTION 361
Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

A. assess the problems and institute rollback procedures, if neede
B. disconnect the systems from the network until the problems are correcte
C. immediately uninstall the patches from these system
D. immediately contact the vendor regarding the problems that occurre

Answer: A

Explanation:

Assessing the problems and instituting rollback procedures as needed would be the best course of action. Choices B and C would not identify where the problem was, and may in fact make the problem worse. Choice D is part of the assessment.

NEW QUESTION 365
What is the PRIMARY objective of a post-event review in incident response?

A. Adjust budget provisioning
B. Preserve forensic data
C. Improve the response process
D. Ensure the incident is fully documented

Answer: C

Explanation:

The primary objective is to find any weakness in the current process and improve it. The other choices are all secondary.

NEW QUESTION 368
Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

A. Preparedness tests
B. Paper tests
C. Full operational tests
D. Actual service disruption

Answer: A

Explanation:

Preparedness tests would involve simulation of the entire test in phases and help the team better understand and prepare for the actual test scenario. Options B, C and D are not cost-effective ways to establish plan effectiveness. Paper tests in a walk-through do not include simulation and so there is less learning and it is difficult to obtain evidence that the team has understood the test plan. Option D is not recommended in most cases. Option C would require an approval from management is not easy or practical to test in most scenarios and may itself trigger a disaster.

NEW QUESTION 372
When creating a forensic image of a hard drive, which of the following should be the FIRST step?

A. Identify a recognized forensics software tool to create the imag
B. Establish a chain of custody lo
C. Connect the hard drive to a write blocke
D. Generate a cryptographic hash of the hard drive content

Answer: B

Explanation:

The first step in any investigation requiring the creation of a forensic image should always be to maintain the chain of custody. Identifying a recognized forensics software tool to create the image is one of the important steps, but it should come after several of the other options. Connecting the hard drive to a write blocker is an important step, but it must be done after the chain of custody has been established. Generating a cryptographic hash of the hard drive contents is another important step, but one that comes after several of the other options.

NEW QUESTION 374
The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

A. enable independent and objective review of the root cause of the incident
B. obtain support for enhancing the expertise of the third-party team
C. identify lessons learned for further improving the information security management proces
D. obtain better buy-in for the information security progra

Answer: A

Explanation:

It is always desirable to avoid the conflict of interest involved in having the information security team carries out the post event review. Obtaining support for enhancing the expertise of the third-party teams is one of the advantages, but is not the primary driver. Identifying lessons learned for further improving the information security management process is the general purpose of carrying out the post event review. Obtaining better buy-in for the information security program is not a valid reason for involving third-party teams.

NEW QUESTION 377
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 378
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

A. Cost to build a redundant processing facility and invocation
B. Daily cost of losing critical systems and recovery time objectives (RTOs)
C. Infrastructure complexity and system sensitivity
D. Criticality results from the business impact analysis (BIA)

Answer: C

Explanation:

The complexity and business sensitivity of the processing infrastructure and operations largely determines the viability of such an option; the concern is whether the recovery site meets the operational and security needs of the organization. The cost to build a redundant facility is not relevant since only a fraction of the total processing capacity is considered critical at the time of the disaster and recurring contract costs would accrue over time. Invocation costs are not a factor because they will be the same regardless. The incremental daily cost of losing different systems and the recovery time objectives (RTOs) do not distinguish whether a commercial facility is chosen. Resulting criticality from the business impact analysis (BIA) will determine the scope and timeline of the recovery efforts, regardless of the recovery location.

NEW QUESTION 380
A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly

over the Internet. Which of the following should be performed FIRST in response to this threat?

A. Quarantine all picture files stored on file servers
B. Block all e-mails containing picture file attachments
C. Quarantine all mail servers connected to the Internet
D. Block incoming Internet mail, but permit outgoing mail

Answer: B

Explanation:

Until signature files can be updated, incoming e-mail containing picture file attachments should be blocked. Quarantining picture files already stored on file servers is not effective since these files must be intercepted before they are opened. Quarantine of all mail servers or blocking all incoming mail is unnecessary overkill since only those e-mails containing attached picture files are in question.

NEW QUESTION 383
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the inciden
B. notify senior managemen
C. start containmen
D. notify law enforcemen

Answer: A

Explanation:

Asserting that the condition is a true security incident is the necessary first step in determining the correct response. The containment stage would follow. Notifying senior management and law enforcement could be part of the incident response process that takes place after confirming an incident.

NEW QUESTION 385
Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

A. Incident response metrics
B. Periodic auditing of the incident response process
C. Action recording and review
D. Post incident review

Answer: D

Explanation:

Post event reviews are designed to identify gaps and shortcomings in the actual incident response process so that these gaps may be improved over time. The other choices will not provide the same level of feedback in improving the process.

NEW QUESTION 388
A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. rebuild the server from the last verified backu
B. place the web server in quarantin
C. shut down the server in an organized manne
D. rebuild the server with original media and relevant patche

Answer: D

Explanation:

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

NEW QUESTION 389
In the course of examining a computer system for forensic evidence, data on the suspect media were inadvertently altered. Which of the following should have been the FIRST course of action in the investigative process?

A. Perform a backup of the suspect media to new medi
B. Perform a bit-by-bit image of the original media source onto new medi
C. Make a copy of all files that are relevant to the investigatio
D. Run an error-checking program on all logical drives to ensure that there are no disk error

Answer: B

Explanation:

The original hard drive or suspect media should never be used as the source for analysis. The source or original media should be physically secured and only used as the master to create a bit-by-bit image. The original should be stored using the appropriate procedures, depending on location. The image created for

forensic analysis should be used. A backup does not preserve 100 percent of the data, such as erased or deleted files and data in slack space—which may be critical to the investigative process. Once data from the source are altered, they may no longer be admissible in court. Continuing the investigation, documenting the date, time and data altered, are actions that may not be admissible in legal proceedings. The organization would need to know the details of collecting and preserving forensic evidence relevant to their jurisdiction.

NEW QUESTION 390
Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite
B. Conduct an assessment to determine system status
C. Perform an impact analysis of the outage
D. Isolate the screened subnet

Answer: B

Explanation:

An assessment should be conducted to determine whether any permanent damage occurred and the overall system status. It is not necessary at this point to rebuild any servers. An impact analysis of the outage or isolating the demilitarized zone (DMZ) or screen subnet will not provide any immediate benefit.

NEW QUESTION 394
An organization has learned of a security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

A. assess the likelihood of incidents from the reported caus
B. discontinue the use of the vulnerable technolog
C. report to senior management that the organization is not affecte
D. remind staff that no similar security breaches have taken plac

Answer: A

Explanation:

The security manager should first assess the likelihood of a similar incident occurring, based on available information. Discontinuing the use of the vulnerable technology would not necessarily be practical since it would likely be needed to support the business. Reporting to senior management that the organization is not affected due to controls already in place would be premature until the information security manager can first assess the impact of the incident. Until this has been researched, it is not certain that no similar security breaches have taken place.

NEW QUESTION 399
When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

A. Assigning responsibility for acquiring the data
B. Locating the data and preserving the integrity of the data
C. Creating a forensically sound image
D. Issuing a litigation hold to all affected parties

Answer: B

Explanation:

Locating the data and preserving data integrity is the only correct answer because it represents the primary responsibility of an investigator and is a complete and accurate statement of the first priority. While assigning responsibility for acquiring the data is a step that should be taken, it is not the first step or the highest priority. Creating a forensically sound image may or may not be a necessary step, depending on the type of investigation, but it would never be the first priority. Issuing a litigation hold to all affected parties might be a necessary step early on in an investigation of certain types, but not the first priority.

NEW QUESTION 401
Which of the following is MOST closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy
C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

Answer: D

Explanation:

Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

NEW QUESTION 403
Which of the following is MOST important in determining whether a disaster recovery test is successful?

A. Only business data files from offsite storage are used
B. IT staff fully recovers the processing infrastructure
C. Critical business processes are duplicated
D. All systems are restored within recovery time objectives (RTOs)

Answer: C

Explanation:

To ensure that a disaster recovery test is successful, it is most important to determine whether all critical business functions were successfully recovered and duplicated. Although ensuring that only materials taken from offsite storage are used in the test is important, this is not as critical in determining a test's success. While full recovery of the processing infrastructure is a key recovery milestone, it does not ensure the success of a test. Achieving the RTOs is another important milestone, but does not necessarily prove that the critical business functions can be conducted, due to interdependencies with other applications and key elements such as data, staff, manual processes, materials and accessories, etc.

NEW QUESTION 405
Of the following, which is the MOST important aspect of forensic investigations?

A. The independence of the investigator
B. Timely intervention
C. Identifying the perpetrator
D. Chain of custody

Answer: D

Explanation:

Establishing the chain of custody is one of the most important steps in conducting forensic investigations since it preserves the evidence in a manner that is admissible in court. The independence of the investigator may be important, but is not the most important aspect. Timely intervention is important for containing incidents, but not as important for forensic investigation. Identifying the perpetrator is important, but maintaining the chain of custody is more important in order to have the perpetrator convicted in court.

NEW QUESTION 407
An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

A. Inform senior managemen
B. Determine the extent of the compromis
C. Report the incident to the authoritie
D. Communicate with the affected customer

Answer: B

Explanation:

Before reporting to senior management, affected customers or the authorities, the extent of the exposure needs to be assessed.

NEW QUESTION 409
The MOST important objective of a post incident review is to:

A. capture lessons learned to improve the proces
B. develop a process for continuous improvemen
C. develop a business case for the security program budge
D. identify new incident management tool

Answer: A

Explanation:

The main purpose of a post incident review is to identify areas of improvement in the process. Developing a process for continuous improvement is not true in every case. Developing a business case for the security program budget and identifying new incident management tools may come from the analysis of the incident, but are not the key objectives.

NEW QUESTION 414
What is the FIRST action an information security manager should take when a company laptop is reported stolen?

A. Evaluate the impact of the information loss
B. Update the corporate laptop inventory
C. Ensure compliance with reporting procedures
D. Disable the user account immediately

Answer: C

Explanation:

The key step in such an incident is to report it to mitigate any loss. After this, the other actions should follow.

NEW QUESTION 415
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts

B. Write access violations
C. Concurrent logons
D. Firewall logs

Answer: A

Explanation:

Since the password for the shared administrative account was obtained through guessing, it is probable that there were multiple unsuccessful logon attempts before the correct password was deduced. Searching the logs for invalid logon attempts could, therefore, lead to the discovery of this unauthorized activity. Because the account is shared, reviewing the logs for concurrent logons would not reveal unauthorized activity since concurrent usage is common in this situation. Write access violations would not necessarily be observed since the information was merely copied and not altered. Firewall logs would not necessarily contain information regarding logon attempts.

NEW QUESTION 419
Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

A. determining the extent of property damag
B. preserving environmental condition
C. ensuring orderly plan activatio
D. reducing the extent of operational damag

Answer: D

Explanation:

During an incident, emergency actions should minimize or eliminate casualties and damage to the business operation, thus reducing business interruptions. Determining the extent of property damage is not the consideration; emergency actions should minimize, not determine, the extent of the damage. Protecting/preserving environmental conditions may not be relevant. Ensuring orderly plan activation is important but not as critical as reducing damage to the operation.

NEW QUESTION 423
A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

A. Risk assessment results
B. Severity criteria
C. Emergency call tree directory
D. Table of critical backup files

Answer: B

Explanation:

Quickly ranking the severity criteria of an incident is a key element of incident response. The other choices refer to documents that would not likely be included in a computer incident response team (CIRT) manual.

NEW QUESTION 424
The BEST approach in managing a security incident involving a successful penetration should be to:

A. allow business processes to continue during the respons
B. allow the security team to assess the attack profil
C. permit the incident to continue to trace the sourc
D. examine the incident response process for deficiencie

Answer: A

Explanation:

Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted. Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable but it, too. is subordinate to allowing business processes to continue.

NEW QUESTION 429
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISM Practice Exam Features:

* CISM Questions and Answers Updated Frequently

* CISM Practice Questions Verified by Expert Senior Certified Staff

* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year