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 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 3
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 4
From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

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

Answer: D

Explanation:

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

NEW QUESTION 5
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

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

Answer: D

Explanation:

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

NEW QUESTION 6
Investments in information security technologies should be based on:

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

Answer: B

Explanation:

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

NEW QUESTION 7
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

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

Answer: B

Explanation:

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

NEW QUESTION 8
When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

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

Answer: D

Explanation:

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

NEW QUESTION 9
Who should be responsible for enforcing access rights to application data?

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

Answer: D

Explanation:

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

NEW QUESTION 10
Which of the following is the MOST important factor when designing information security architecture?

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

Answer: D

Explanation:

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

NEW QUESTION 10
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Answer: C

Explanation:

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

NEW QUESTION 13
Which of the following are likely to be updated MOST frequently?

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

Answer: A

Explanation:

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

NEW QUESTION 17
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

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

Answer: B

Explanation:

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

NEW QUESTION 19
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 24
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 25
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 26
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

A. establishing a periodic risk assessmen
B. promoting regulatory requirement
C. developing a business cas
D. developing effective metric

Answer: C

Explanation:

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

NEW QUESTION 27
A good privacy statement should include:

A. notification of liability on accuracy of informatio
B. notification that information will be encrypte
C. what the company will do with information it collect
D. a description of the information classification proces

Answer: C

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. Choice A is incorrect because that information should be located in the web site's disclaimer. Choice B is incorrect because, although encryption may be applied, this is not generally disclosed. Choice D is incorrect because information classification would be contained in a separate policy.

NEW QUESTION 32
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

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

Answer: C

Explanation:

Strategic alignment of security with business objectives is a key indicator of performance measurement. In guiding a security program, a meaningful performance measurement will also rely on an understanding of business objectives, which will be an outcome of alignment. Business linkages do not by themselves indicate

integration or value delivery. While alignment is an important precondition, it is not as important an indicator.

NEW QUESTION 33
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

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

Answer: D

Explanation:

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

NEW QUESTION 35
What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

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

Answer: D

Explanation:

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

NEW QUESTION 36
Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

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

Answer: C

Explanation:

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

NEW QUESTION 41
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 42
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

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

Answer: A

Explanation:

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

NEW QUESTION 45
Which of the following requirements would have the lowest level of priority in information security?

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

Answer: A

Explanation:

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

NEW QUESTION 50
When developing an information security program, what is the MOST useful source of information for determining available resources?

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

Answer: D

Explanation:

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

NEW QUESTION 55
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 56
Which of the following should be determined while defining risk management strategies?

A. Risk assessment criteria
B. Organizational objectives and risk appetite
C. IT architecture complexity
D. Enterprise disaster recovery plans

Answer: B

Explanation:

While defining risk management strategies, one needs to analyze the organization's objectives and risk appetite and define a risk management framework based on this analysis. Some organizations may accept known risks, while others may invest in and apply mitigation controls to reduce risks. Risk assessment criteria would become part of this framework, but only after proper analysis. IT architecture complexity and enterprise disaster recovery plans are more directly related to assessing risks than defining strategies.

NEW QUESTION 61
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 62
Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

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

Answer: D

Explanation:

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

NEW QUESTION 67
Senior management commitment and support for information security can BEST be enhanced through:

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

Answer: C

Explanation:

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

NEW QUESTION 68
Information security projects should be prioritized on the basis of:

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

Answer: BExplanation:

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

NEW QUESTION 71
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 73
The cost of implementing a security control should not exceed the:

A. annualized loss expectanc
B. cost of an inciden
C. asset valu
D. implementation opportunity cost

Answer: C

Explanation:

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses drat are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

NEW QUESTION 77
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 80
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 83
To determine the selection of controls required to meet business objectives, an information security manager should:

A. prioritize the use of role-based access control
B. focus on key control
C. restrict controls to only critical application
D. focus on automated control

Answer: B

Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

NEW QUESTION 85
The PRIMARY purpose of using risk analysis within a security program is to:

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

Answer: D

Explanation:

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

NEW QUESTION 86
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

A. a lack of proper input validation control
B. weak authentication controls in the web application laye
C. flawed cryptographic secure sockets layer (SSL) implementations and short key length
D. implicit web application trust relationship

Answer: A

Explanation:

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

NEW QUESTION 90
The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

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

Answer: A

Explanation:

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

NEW QUESTION 95
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 97
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 102
The recovery point objective (RPO) requires which of the following?

A. Disaster declaration
B. Before-image restoration
C. System restoration
D. After-image processing

Answer: B

Explanation:

The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application

processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

NEW QUESTION 104
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 107
Risk assessment is MOST effective when performed:

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

Answer: B

Explanation:

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

NEW QUESTION 111
An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

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

Answer: C

Explanation:

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

NEW QUESTION 115
Which of the following are the essential ingredients of a business impact analysis (B1A)?

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

Answer: A

Explanation:

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

NEW QUESTION 120
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

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

Answer: B

Explanation:

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

NEW QUESTION 123
To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

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

Answer: D

Explanation:

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

NEW QUESTION 127
Which of the following would generally have the GREATEST negative impact on an organization?

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

Answer: C

Explanation:

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

NEW QUESTION 131
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 134
The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

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

Answer: D

Explanation:

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

NEW QUESTION 139
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

A. External auditors

B. A peer group within a similar business
C. Process owners
D. A specialized management consultant

Answer: C

Explanation:

Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties do not have that level of detailed knowledge on the inner workings of the business. Management consultants are expected to have the necessary skills in risk analysis techniques but are still less effective than a group with intimate knowledge of the business.

NEW QUESTION 144
There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

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

Answer: A

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

NEW QUESTION 145
Which of the following would help management determine the resources needed to mitigate a risk to the organization?

A. Risk analysis process
B. Business impact analysis (BIA)
C. Risk management balanced scorecard
D. Risk-based audit program

Answer: B

Explanation:

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

NEW QUESTION 149
When implementing security controls, an information security manager must PRIMARILY focus on:

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

Answer: A

Explanation:

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

NEW QUESTION 152
Which of the following BEST indicates a successful risk management practice?

A. Overall risk is quantified
B. Inherent risk is eliminated
C. Residual risk is minimized
D. Control risk is tied to business units

Answer: C

Explanation:

A successful risk management practice minimizes the residual risk to the organization. Choice A is incorrect because the fact that overall risk has been quantified does not necessarily indicate the existence of a successful risk management practice. Choice B is incorrect since it is virtually impossible to eliminate inherent risk. Choice D is incorrect because, although the tying of control risks to business may improve accountability, this is not as desirable as minimizing residual risk.

NEW QUESTION 153
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 154
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

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

Answer: C

Explanation:

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

NEW QUESTION 157
Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

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

Answer: D

Explanation:

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

NEW QUESTION 160
Which of the following will BEST prevent external security attacks?

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

Answer: B

Explanation:

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

NEW QUESTION 163
In assessing risk, it is MOST essential to:

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

Answer: C

Explanation:

A risk analysis should take into account the potential financial impact and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus

primarily on recent losses or losses experienced by similar firms. Although this is important supplementary information, it does not reflect the organization's real situation. Geography and other factors come into play as well.

NEW QUESTION 165
Which of the following risks is represented in the risk appetite of an organization?

A. Control
B. Inherent
C. Residual
D. Audit

Answer: C

Explanation:

Residual risk is unmanaged, i.e., inherent risk which remains uncontrolled. This is key to the organization's risk appetite and is the amount of residual risk that a business is living with that affects its viability. Hence, inherent risk is incorrect. Control risk, the potential for controls to fail, and audit risk, which relates only to audit's approach to their work, are not relevant in this context.

NEW QUESTION 168
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 170
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

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

Answer: C

Explanation:

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

NEW QUESTION 173
Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

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

Answer: B

Explanation:

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

NEW QUESTION 175
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 180
Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

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

Answer: B

Explanation:

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

NEW QUESTION 182
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

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

Answer: D

Explanation:

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

NEW QUESTION 187
A digital signature using a public key infrastructure (PKI) will:

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

Answer: B

Explanation:

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

NEW QUESTION 192
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

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

Answer: A

Explanation:

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

NEW QUESTION 197
The MAIN advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workloa
B. increases security between multi-tier system
C. allows passwords to be changed less frequentl

D. reduces the need for two-factor authenticatio

Answer: A

Explanation:

Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multi-tier systems, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

NEW QUESTION 198
Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

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

Answer: D

Explanation:

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

NEW QUESTION 200
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 205
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

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

Answer: C

Explanation:

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

NEW QUESTION 210
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 211
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

A. an adequate budget for the security progra

B. recruitment of technical IT employee
C. periodic risk assessment
D. security awareness training for employee

Answer: D

Explanation:

An information security manager has to impress upon the human resources department the need for security awareness training for all employees. Budget considerations are more of an accounting function. The human resources department would become involved once they are convinced for the need of security awareness training. Recruiting IT-savvy staff may bring in new employees with better awareness of information security, but that is not a replacement for the training requirements of the other employees. Periodic risk assessments may or may not involve the human resources department function.

NEW QUESTION 215
Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

A. Patch management
B. Change management
C. Security baselines
D. Virus detection

Answer: B

Explanation:
Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses. Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

NEW QUESTION 219
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

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

Answer: B

Explanation:

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

NEW QUESTION 221
An e-commerce order fulfillment web server should generally be placed on which of the following?

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

Answer: B

Explanation:

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

NEW QUESTION 224
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

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

Answer: B

Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the

receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and. second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

NEW QUESTION 226
Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

Answer: C

Explanation:

Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

NEW QUESTION 230
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 231
Nonrepudiation can BEST be ensured by using:

A. strong password
B. a digital has
C. symmetric encryptio
D. digital signature

Answer: D

Explanation:

Digital signatures use a private and public key pair, authenticating both parties. The integrity of the contents exchanged is controlled through the hashing mechanism that is signed by the private key of the exchanging party. A digital hash in itself helps in ensuring integrity of the contents, but not nonrepudiation. Symmetric encryption wouldn't help in nonrepudiation since the keys are always shared between parties. Strong passwords only ensure authentication to the system and cannot be used for nonrepudiation involving two or more parties.

NEW QUESTION 235
Access control to a sensitive intranet application by mobile users can BEST be implemented through:

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

Answer: D

Explanation:

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

NEW QUESTION 240
Which of the following devices should be placed within a DMZ?

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

Answer: C

Explanation:

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

NEW QUESTION 242
The MOST important success factor to design an effective IT security awareness program is to:

A. customize the content to the target audienc
B. ensure senior management is represente
C. ensure that all the staff is traine
D. avoid technical content but give concrete example

Answer: A

Explanation:

Awareness training can only be effective if it is customized to the expectations and needs of attendees. Needs will be quite different depending on the target audience and will vary between business managers, end users and IT staff; program content and the level of detail communicated will therefore be different. Other criteria are also important; however, the customization of content is the most important factor.

NEW QUESTION 245
Which of the following would be the BEST defense against sniffing?

A. Password protect the files
B. Implement a dynamic IP address scheme
C. Encrypt the data being transmitted
D. Set static mandatory access control (MAC) addresses

Answer: C

Explanation:

Encrypting the data will obfuscate the data so that they are not visible in plain text. Someone would have to collate the entire data stream and try decrypting it, which is not easy. Passwords can be recovered by brute-force attacks and by password crackers, so this is not the best defense against sniffing. IP addresses can always be discovered, even if dynamic IP addresses are implemented. The person sniffing traffic can initiate multiple sessions for possible IP addresses. Setting static mandatory access control (MAC) addresses can prevent address resolution protocol (ARP) poisoning, but it does not prevent sniffing.

NEW QUESTION 249
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 250
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 255
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager
B. Establish predetermined automatic expiration dates

C. Require managers to e-mail security when the user leaves
D. Ensure each individual has signed a security acknowledgement

Answer: B

Explanation:

Predetermined expiration dates are the most effective means of removing systems access for temporary users. Reliance on managers to promptly send in termination notices cannot always be counted on, while requiring each individual to sign a security acknowledgement would have little effect in this case.

NEW QUESTION 256
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

A. contribute cost-effective expertise not available internall
B. be made responsible for meeting the security program requirement
C. replace the dependence on internal resource
D. deliver more effectively on account of their knowledg

Answer: A

Explanation:

Choice A represents the primary driver for the information security manager to make use of external resources. The information security manager will continue to be responsible for meeting the security program requirements despite using the services of external resources. The external resources should never completely replace the role of internal resources from a strategic perspective. The external resources cannot have a better knowledge of the business of the information security manager's organization than do the internal resources.

NEW QUESTION 260
Security awareness training is MOST likely to lead to which of the following?

A. Decrease in intrusion incidents
B. Increase in reported incidents
C. Decrease in security policy changes
D. Increase in access rule violations

Answer: B

Explanation:

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

NEW QUESTION 264
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 268
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 273
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 278
Which of the following devices should be placed within a DMZ?

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

Answer: B

Explanation:

An application server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Data warehouse and departmental servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. A proxy server forms the inner boundary of the DMZ but is not placed within it.

NEW QUESTION 279
An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RI P) is the:

A. references from other organization
B. past experience of the engagement tea
C. sample deliverabl
D. methodology used in the assessmen

Answer: D

Explanation:

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

NEW QUESTION 280
Which of the following is the BEST indicator that an effective security control is built into an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 285
Which of the following areas is MOST susceptible to the introduction of security weaknesses?

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

Answer: C

Explanation:

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

NEW QUESTION 286
Which would be the BEST recommendation to protect against phishing attacks?

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

Answer: B

Explanation:

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

NEW QUESTION 288
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 293
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 294
Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

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

Answer: A

Explanation:

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

NEW QUESTION 297
An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

A. Right to audit
B. Nondisclosure agreement
C. Proper firewall implementation
D. Dedicated security manager for monitoring compliance

Answer: A

Explanation:

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a

business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

NEW QUESTION 301
The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

A. identifying vulnerabilities in the syste
B. sustaining the organization's security postur
C. the existing systems that will be affecte
D. complying with segregation of dutie

Answer: B

Explanation:

It is important to maintain the organization's security posture at all times. The focus should not be confined to the new system being developed or acquired, or to the existing systems in use. Segregation of duties is only part of a solution to improving the security of the systems, not the primary reason to involve security in the systems development life cycle (SDLC).

NEW QUESTION 304
Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

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

Answer: C

Explanation:

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

NEW QUESTION 307
Security policies should be aligned MOST closely with:

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

Answer: B

Explanation:

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

NEW QUESTION 310
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

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

Answer: B

Explanation:

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

NEW QUESTION 311
What is the MOST important success factor in launching a corporate information security awareness program?

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

Answer:

C

Explanation:

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

NEW QUESTION 316
Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

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

Answer: A

Explanation:

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

NEW QUESTION 319
What is the BEST way to ensure users comply with organizational security requirements for password complexity?

A. Include password construction requirements in the security standards
B. Require each user to acknowledge the password requirements
C. Implement strict penalties for user noncompliance
D. Enable system-enforced password configuration

Answer: D

Explanation:

Automated controls are generally more effective in preventing improper actions. Policies and standards provide some deterrence, but are not as effective as automated controls.

NEW QUESTION 323
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 326
Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection syste
B. Establish minimum security baseline
C. Implement vendor recommended setting
D. Perform periodic penetration testin

Answer: D

Explanation:

Penetration testing is the best way to assure that perimeter security is adequate. An intrusion detection system (IDS) may detect an attempted attack, hut it will not confirm whether the perimeter is secured. Minimum security baselines and applying vendor recommended settings are beneficial, but they will not provide the level of assurance that is provided by penetration testing.

NEW QUESTION 330
Which of the following BEST ensures that security risks will be reevaluated when modifications in application developments are made?

A. A problem management process
B. Background screening
C. A change control process
D. Business impact analysis (BIA)

Answer: C

Explanation:

A change control process is the methodology that ensures that anything that could be impacted by a development change will be reevaluated. Problem management is the general process intended to manage all problems, not those specifically related to security. Background screening is the process to evaluate employee references when they are hired. BIA is the methodology used to evaluate risks in the business continuity process.

NEW QUESTION 335
Successful social engineering attacks can BEST be prevented through:

A. preemployment screenin
B. close monitoring of users' access pattern
C. periodic awareness trainin
D. efficient termination procedure

Answer: C

Explanation:

Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

NEW QUESTION 336
Which of the following presents the GREATEST exposure to internal attack on a network?

A. User passwords are not automatically expired
B. All network traffic goes through a single switch
C. User passwords are encoded but not encrypted
D. All users reside on a single internal subnet

Answer: C

Explanation:

When passwords are sent over the internal network in an encoded format, they can easily be converted to clear text. All passwords should be encrypted to provide adequate security. Not automatically expiring user passwords does create an exposure, but not as great as having unencrypted passwords. Using a single switch or subnet does not present a significant exposure.

NEW QUESTION 341
Nonrepudiation can BEST be assured by using:

A. delivery path tracin
B. reverse lookup translatio
C. out-of-hand channel
D. digital signature

Answer: D

Explanation:

Effective nonrepudiation requires the use of digital signatures. Reverse lookup translation involves converting Internet Protocol (IP) addresses to usernames. Delivery path tracing shows the route taken but does not confirm the identity of the sender. Out-of-band channels are useful when, for confidentiality, it is necessary to break a message into two parts that are sent by different means.

NEW QUESTION 345
Of the following, retention of business records should be PRIMARILY based on:

A. periodic vulnerability assessmen
B. regulatory and legal requirement
C. device storage capacity and longevit
D. past litigatio

Answer: B

Explanation:

Retention of business records is a business requirement that must consider regulatory and legal requirements based on geographic location and industry. Options A and C are important elements for making the decision, but the primary driver is the legal and regulatory requirements that need to be followed by all companies. Record retention may take into consideration past litigation, but it should not be the primary decision factor.

NEW QUESTION 348

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 352
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 356
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 359
Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

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

Answer: D

Explanation:

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

NEW QUESTION 363
Who is responsible for raising awareness of the need for adequate funding for risk action plans?

A. Chief information officer (CIO)
B. Chief financial officer (CFO)
C. Information security manager
D. Business unit management

Answer: C

Explanation:

The information security manager is responsible for raising awareness of the need for adequate funding for risk-related action plans. Even though the chief information officer (CIO), chief financial officer (CFO) and business unit management are involved in the final approval of fund expenditure, it is the information security manager who has the ultimate responsibility for raising awareness.

NEW QUESTION 364
The PRIMARY objective of security awareness is to:

A. ensure that security policies are understoo
B. influence employee behavio
C. ensure legal and regulatory compliance
D. notify of actions for noncomplianc

Answer: B

Explanation:

It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, or meeting legal and regulatory requirements is important but secondary.

NEW QUESTION 367
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 370
Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m. (23.00 hrs.)?

A. Most new viruses* signatures are identified over weekends
B. Technical personnel are not available to support the operation
C. Systems are vulnerable to new viruses during the intervening week
D. The update's success or failure is not known until Monday

Answer: C

Explanation:

Updating virus signature files on a weekly basis carries the risk that the systems will be vulnerable to viruses released during the week; far more frequent updating is essential. All
other issues are secondary to this very serious exposure.

NEW QUESTION 373
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 377
Which of the following is the BEST way to verify that all critical production servers are utilizing up-to- date virus signature files?

A. Verify the date that signature files were last pushed out
B. Use a recently identified benign virus to test if it is quarantined
C. Research the most recent signature file and compare to the console
D. Check a sample of servers that the signature files are current

Answer: D

Explanation:

The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that il was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

NEW QUESTION 379
A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

A. document how the attack occurre
B. notify law enforcemen
C. take an image copy of the medi
D. close the accounts receivable syste

Answer: C

Explanation:

Taking an image copy of the media is a recommended practice to ensure legal admissibility. All of the other choices are subsequent and may be supplementary.

NEW QUESTION 384
The PRIORITY action to be taken when a server is infected with a virus is to:

A. isolate the infected server(s) from the networ
B. identify all potential damage caused by the infectio
C. ensure that the virus database files are curren
D. establish security weaknesses in the firewal

Answer: A

Explanation:

The priority in this event is to minimize the effect of the virus infection and to prevent it from spreading by removing the infected server(s) from the network. After the network is secured from further infection, the damage assessment can be performed, the virus database updated and any weaknesses sought.

NEW QUESTION 387
A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

A. Run a port scan on the system
B. Disable the logon ID
C. Investigate the system logs
D. Validate the incident

Answer: D

Explanation:

When investigating a possible incident, it should first be validated. Running a port scan on the system, disabling the logon IDs and investigating the system logs may be required based on preliminary forensic investigation, but doing so as a first step may destroy the evidence.

NEW QUESTION 391
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 393
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 397
In the course of responding 10 an information security incident, the BEST way to treat evidence for possible legal action is defined by:

A. international standard
B. local regulation
C. generally accepted best practice
D. organizational security policie

Answer: B

Explanation:

Legal follow-up will most likely be performed locally where the incident took place; therefore, it is critical that the procedure of treating evidence is in compliance with local regulations. In certain countries, there are strict regulations on what information can be collected. When evidence collected is not in compliance with local regulations, it may not be admissible in court. There are no common regulations to treat computer evidence that are accepted internationally. Generally accepted best practices such as a common chain-of-custody concept may have different implementation in different countries, and thus may not be a good assurance that evidence will be admissible. Local regulations always take precedence over organizational security policies.

NEW QUESTION 402
What task should be performed once a security incident has been verified?

A. Identify the inciden
B. Contain the inciden
C. Determine the root cause of the inciden
D. Perform a vulnerability assessmen

Answer: B

Explanation:

Identifying the incident means verifying whether an incident has occurred and finding out more details about the incident. Once an incident has been confirmed (identified), the incident management team should limit further exposure. Determining the root cause takes place after the incident has been contained. Performing a vulnerability assessment takes place after the root cause of an incident has been determined, in order to find new vulnerabilities.

NEW QUESTION 406
The PRIMARY purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

A. weaknesses in network and server securit
B. ways to improve the incident response proces
C. potential attack vectors on the network perimete
D. the optimum response to internal hacker attack

Answer: A

Explanation:

An internal attack and penetration test are designed to identify weaknesses in network and server security. They do not focus as much on incident response or the network perimeter.

NEW QUESTION 410
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 413

Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

A. Setting up a backup site
B. Maintaining redundant systems
C. Aligning with recovery time objectives (RTOs)
D. Data backup frequency

Answer: C

Explanation:

BCP.'DRP should align with business RTOs. The RTO represents the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RTO must be taken into consideration when prioritizing systems for recovery efforts to ensure that those systems that the business requires first are the ones that are recovered first.

NEW QUESTION 415
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 420
When collecting evidence for forensic analysis, it is important to:

A. ensure the assignment of qualified personne
B. request the IT department do an image cop
C. disconnect from the network and isolate the affected device
D. ensure law enforcement personnel are present before the forensic analysis commence

Answer: A

Explanation:

Without the initial assignment of forensic expertise, the required levels of evidence may not
be preserved. In choice B. the IT department is unlikely to have that level of expertise and should, thus, be prevented from taking action. Choice C may be a subsequent necessity that comes after choice A. Choice D, notifying law enforcement, will likely occur after the forensic analysis has been completed.

NEW QUESTION 425
An organization with multiple data centers has designated one of its own facilities as the recovery site. The MOST important concern is the:

A. communication line capacity between data center
B. current processing capacity loads at data center
C. differences in logical security at each cente
D. synchronization of system software release version

Answer: B

Explanation:

If data centers are operating at or near capacity, it may prove difficult to recover critical operations at an alternate data center. Although line capacity is important from a mirroring perspective, this is secondary to having the necessary capacity to restore critical systems. By comparison, differences in logical and physical security and synchronization of system software releases are much easier issues to overcome and are, therefore, of less concern.

NEW QUESTION 430
An incident response policy must contain:

A. updated call tree
B. escalation criteri
C. press release template
D. critical backup files inventor

Answer: B

Explanation:

Escalation criteria, indicating the circumstances under which specific actions are to be undertaken, should be contained within an incident response policy. Telephone trees, press release templates and lists of critical backup files are too detailed to be included in a policy document.

NEW QUESTION 434

Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

A. A hot site facility will be shared in multiple disaster declarations
B. All equipment is provided "at time of disaster, not on floor"
C. The facility is subject to a "first-come, first-served" policy
D. Equipment may be substituted with equivalent model

Answer: B

Explanation:

Equipment provided "at time of disaster (ATOD), not on floor" means that the equipment is not available but will be acquired by the commercial hot site provider ON a best effort basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations, and that priority may be established on a first-come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

NEW QUESTION 439
Detailed business continuity plans should be based PRIMARILY on:

A. consideration of different alternative
B. the solution that is least expensiv
C. strategies that cover all application
D. strategies validated by senior managemen

Answer: D

Explanation:

A recovery strategy identifies the best way to recover a system in ease of disaster and provides guidance based on detailed recovery procedures that can be developed. Different strategies should be developed and all alternatives presented to senior management. Senior management should select the most appropriate strategy from the alternatives provided. The selected strategy should be used for further development of the detailed business continuity plan. The selection of strategy depends on criticality of the business process and applications supporting the processes. It need not necessarily cover all applications. All recovery strategies have associated costs, which include costs of preparing for disruptions and putting them to use in the event of a disruption. The latter can be insured against, but not the former. The best recovery option need not be the least expensive.

NEW QUESTION 443
The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

A. weaknesses in network securit
B. patterns of suspicious acces
C. how an attack was launched on the networ
D. potential attacks on the internal networ

Answer: D

Explanation:

The most important function of an intrusion detection system (IDS) is to identify potential attacks on the network. Identifying how the attack was launched is secondary. It is not designed specifically to identify weaknesses in network security or to identify patterns of suspicious logon attempts.

NEW QUESTION 444
.....

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