Passguide CISM 468q

Number: CISM
Passing Score: 800
Time Limit: 120 min
File Version: 16.5

Isaca CISM

Certified Information Security Manager

Excellent Questions, I pass with 90% with these questions. Guys just read this only.Good luck for success.

Exam A

QUESTION 1
Which of the following should be the FIRST step in developing an information security plan?

A. Perform a technical vulnerabilities assessment
B. Analyze the current business strategy
C. Perform a business impact analysis
D. Assess the current levels of security awareness

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

QUESTION 2
Senior management commitment and support for information security can BEST be obtained through presentations that:

A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best security practices.
D. tie security risks to key business objectives.

Correct Answer: D
Section: (none)
Explanation

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

Real 2
Isaca CISM Exam

QUESTION 3
The MOST appropriate role for senior management in supporting information security is the:

A. evaluation of vendors offering security products.
B. assessment of risks to the organization.
C. approval of policy statements and funding.
D. monitoring adherence to regulatory requirements.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since the members of senior management are ultimately responsible for information security, they are the

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

QUESTION 4
Investments in information security technologies should be based on:

A. vulnerability assessments.
   Real 4
   Isaca CISM Exam
B. value analysis.
C. business climate.
D. audit recommendations.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 5
Retention of business records should PRIMARILY be based on:

A. business strategy and direction.
B. regulatory and legal requirements.
C. storage capacity and longevity.
D. business ease and value analysis.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 6
Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Real 5

Isaca CISM Exam

Explanation:
Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economics of scale. However, turnaround can be slower due to the lack of alignment with business units.

QUESTION 7
Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The chief operating officer (COO) is highly-placed within an organization and has the most knowledge of business operations and objectives. The chief internal auditor and chief legal

Real 6
Isaca CISM Exam

counsel are appropriate members of such a steering group. However, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since a security manager is looking to this group for direction, they are not in the best position to oversee formation of this group.

QUESTION 8
The cost of implementing a security control should not exceed the:

A. annualized loss expectancy.
B. cost of an incident.
C. asset value.
D. implementation opportunity costs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Real 7
Isaca CISM Exam

QUESTION 9
Minimum standards for securing the technical infrastructure should be defined in a security:

A. strategy.
B. guidelines.

C. model.
D. architecture.

Correct Answer: D
Section: (none)
Explanation

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

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

A. organizational risk.
B. organization wide metrics.
C. security needs.
D. the responsibilities of organizational units.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 11
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 vacancies.
B. The chief information officer (CIO) approves security policy changes.
C. The information security oversight committee only meets quarterly.
D. The data center manager has final signoff on all security projects.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Real 10
Isaca CISM Exam

QUESTION 12
Which of the following requirements would have the lowest level of priority in information security?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 13
Which of the following is MOST likely to be discretionary?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 14
Security technologies should be selected PRIMARILY on the basis of their:

A. ability to mitigate business risks.
B. evaluations in trade publications.
C. use of new and emerging technologies.
D. benefits in comparison to their costs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Real 12
Isaca CISM Exam

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

QUESTION 15
Which of the following are seldom changed in response to technological changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

QUESTION 16
Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

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

Correct Answer: B
Section: (none)
Explanation

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

influence across the organization.

QUESTION 17
Relationships among security technologies are BEST defined through which of the following?

A. Security metrics
B. Network topology
C. Security architecture
D. Process improvement models

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security architecture explains the use and relationships of security mechanisms. Security metrics measure improvement within the security practice but do not explain the use and relationships of security technologies. Process improvement models and network topology diagrams also do not describe the use

and relationships of these technologies.

Real 15
Isaca CISM Exam

QUESTION 18
A business unit intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should an information security manager take?

A. Enforce the existing security standard
B. Change the standard to permit the deployment
C. Perform a risk analysis to quantify the risk
D. Perform research to propose use of a better technology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Resolving conflicts of this type should be based on a sound risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. A blanket decision should never be given without conducting such an analysis. Enforcing existing standards is a good practice; however, standards need to be continuously examined in light of new technologies and the risks they present. Standards should not be changed without an appropriate risk assessment.

QUESTION 19
The PRIMARY goal in developing an information security strategy is to:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 20
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 employees.
C. periodic review of alignment with business management goals.
D. senior management signoff on the information security strategy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 21
Which of the following MOST commonly falls within the scope of an information security governance steering committee?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 22
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
Real 18
Isaca CISM Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 23
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 24
The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

A. head of internal audit.
B. chief operations officer (COO).
C. chief technology officer (CTO).
D. legal counsel.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The chief information security officer (CISO) should ideally report to as high a level within the organization as possible. Among the choices given, the chief operations officer (COO) would have not only the appropriate level but also the knowledge of day-to-day operations. The head of internal audit and legal counsel would make good secondary choices, although they would not be as knowledgeable of the operations. Reporting to the chief technology officer (CTO) could become problematic as the CTO's goals for the infrastructure might, at times, run counter to the goals of information security.

Real 20
Isaca CISM Exam

QUESTION 25
Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 26
Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

A. assessing the frequency of incidents.
B. quantifying the cost of control failures.
C. calculating return on investment (ROD projections.
D. comparing spending against similar organizations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Real 21
Isaca CISM Exam

QUESTION 27
Information security projects should be prioritized on the basis of:

A. time required for implementation.
B. impact on the organization.
Real 22
Isaca CISM Exam
C. total cost for implementation.
D. mix of resources required.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 28
Which of the following is the MOST important information to include in an information security standard?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 29
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach--forcing all

locations to be in compliance with the regulations places an undue burden on those locations.

QUESTION 30
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 31
Reviewing which of the following would BEST ensure that security controls are effective?

A. Risk assessment policies
B. Return on security investment
C. Security metrics
D. User access rights

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reviewing security metrics provides senior management a snapshot view and trends of an organization's security posture. Choice A is incorrect because reviewing risk assessment policies would not ensure that the controls are actually working. Choice B is incorrect because reviewing returns on security investments provides business justifications in implementing controls, but does not measure effectiveness of the control itself. Choice D is incorrect because reviewing user access rights is a joint responsibility of the data custodian and the data owner, and does not measure control effectiveness.

QUESTION 32
Which of the following is responsible for legal and regulatory liability?

A. Chief security officer (CSO)
B. Chief legal counsel (CLC)
C. Board and senior management
D. Information security steering group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

Real 26
Isaca CISM Exam

QUESTION 33
Information security policy enforcement is the responsibility of the:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 34
A good privacy statement should include:

A. notification of liability on accuracy of information.
B. notification that information will be encrypted.
C. what the company will do with information it collects.
D. a description of the information classification process.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 35
Which of the following would be MOST effective in successfully implementing restrictive password policies?

Real 28
Isaca CISM Exam

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around

them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

QUESTION 36
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

Real 29
Isaca CISM Exam

A. corporate data privacy policy.
B. data privacy policy where data are collected.
C. data privacy policy of the headquarters' country.
D. data privacy directive applicable globally.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 37
The PRIMARY objective of a security steering group is to:

A. ensure information security covers all business functions.
Real 30
Isaca CISM Exam
B. ensure information security aligns with business goals.
C. raise information security awareness across the organization.
D. implement all decisions on security management across the organization.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 38
At what stage of the applications development process should the security department initially become involved?

Real 31
Isaca CISM Exam

A. When requested

B. At testing
C. At programming
D. At detail requirements

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 39
A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

A. Examples of genuine incidents at similar organizations
B. Statement of generally accepted best practices
C. Associating realistic threats to corporate objectives
D. Analysis of current technological exposures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Linking realistic threats to key business objectives will direct executive attention to them. All other options are supportive but not of as great a value as choice C when trying to obtain the funds for a new program.

QUESTION 40
An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

A. ensure that security processes are consistent across the organization.
B. enforce baseline security levels across the organization.
C. ensure that security processes are fully documented.
D. implement monitoring of key performance indicators for security processes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 33
Isaca CISM Exam

The organization first needs to move from ad hoc to repeatable processes. The organization then needs to document the processes and implement process monitoring and measurement. Baselining security levels will not necessarily assist in process improvement since baselining focuses primarily on control improvement. The organization needs to standardize processes both before documentation, and before monitoring and measurement.

QUESTION 41
Who in an organization has the responsibility for classifying information?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 42
Which of the following is MOST important in developing a security strategy?

A. Creating a positive business security environment
B. Understanding key business objectives
C. Having a reporting line to senior management
D. Allocating sufficient resources to information security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

Real 35
Isaca CISM Exam

QUESTION 43
Who is ultimately responsible for the organization's information?

A. Data custodian
B. Chief information security officer (CISO)
C. Board of directors
D. Chief information officer (CIO)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The board of directors is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. The data custodian is responsible for the maintenance and protection of data. This role is usually filled by the IT department. The chief information security officer (CISO) is responsible for security and carrying out senior management's directives. The chief information officer (CIO) is responsible for information technology within the organization and is not ultimately responsible for the organization's information.

QUESTION 44
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

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

Correct Answer: D
Section: (none)
Explanation

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

Real 36
Isaca CISM Exam

QUESTION 45
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Real 37
Isaca CISM Exam

QUESTION 46
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

A. prepare a security budget.
B. conduct a risk assessment.
C. develop an information security policy.
D. obtain benchmarking information.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 47
An outcome of effective security governance is:

Real 39
Isaca CISM Exam

A. business dependency assessment
B. strategic alignment.
C. risk assessment.
D. planning.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 48
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

A. Give organization standards preference over local regulations
B. Follow local regulations only
C. Make the organization aware of those standards where local regulations causes conflicts
D. Negotiate a local version of the organization standards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Adherence to local regulations must always be the priority. Not following local regulations can prove detrimental to the group organization. Following local regulations only is incorrect since there needs to be some recognition of organization requirements. Making an organization aware of standards is a sensible step, but is not a total solution. Negotiating a local version of the organization standards is the most effective compromise in this situation.

QUESTION 49
The FIRST step in developing an information security management program is to:

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 50
To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

A. Security breach frequency
B. Annualized loss expectancy (ALE)
C. Cost-benefit analysis
D. Peer group comparison

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cost-benefit analysis is the legitimate way to justify budget. The frequency of security breaches may assist the argument for budget but is not the key tool; it does not address the impact. Annualized loss expectancy (ALE) does not address the potential benefit of security investment.

Real 42
Isaca CISM Exam

Peer group comparison would provide a good estimate for the necessary security budget but it would not take into account the specific needs of the organization.

QUESTION 51
Which of the following situations would MOST inhibit the effective implementation of security governance:

A. The complexity of technology
B. Budgetary constraints
C. Conflicting business priorities
D. High-level sponsorship

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The need for senior management involvement and support is a key success factor for the implementation of appropriate security governance. Complexity of technology, budgetary constraints and conflicting business priorities are realities that should be factored into the governance model of the organization, and should not be regarded as inhibitors.

QUESTION 52
What would be the MOST significant security risks when using wireless local area network (LAN) technology?

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

Correct Answer: C

Section: (none)
Explanation

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

QUESTION 53
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

A. performance measurement.
B. integration.
C. alignment.
D. value delivery.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 54
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?

Real 45
Isaca CISM Exam

A. Compliance with international security standards.
B. Use of a two-factor authentication system.
C. Existence of an alternate hot site in case of business disruption.
D. Compliance with the organization's information security requirements.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 55
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

A. review the functionalities and implementation requirements of the solution.
B. review comparison reports of tool implementation in peer companies.

C. provide examples of situations where such a tool would be useful.
D. substantiate the investment in meeting organizational needs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Any investment must be reviewed to determine whether it is cost effective and supports the organizational strategy. It is important to review the features and functionalities provided by such a tool, and to provide examples of situations where the tool would be useful, but that comes after substantiating the investment and return on investment to the organization.

QUESTION 56
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions
Real 47
Isaca CISM Exam
C. Organization chart
D. Skills inventory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 57
The MOST important characteristic of good security policies is that they:

A. state expectations of IT management.
B. state only one general security mandate.
C. are aligned with organizational goals.
D. govern the creation of procedures and guidelines.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 58
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 resolution.
B. ensure that senior management provides authority for security to address the issues.
C. insist that managers or units not in agreement with the security solution accept the risk.
D. refer the issues to senior management along with any security recommendations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 59
Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

A. Include security responsibilities in the job description
B. Require the administrator to obtain security certification
C. Train the system administrator on penetration testing and vulnerability assessment
D. Train the system administrator on risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

QUESTION 60
Which of the following is the MOST important element of an information security strategy?

A. Defined objectives
B. Time frames for delivery
   Real 50
   Isaca CISM Exam
C. Adoption of a control framework
D. Complete policies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Without defined objectives, a strategy--the plan to achieve objectives--cannot be developed. Time frames for delivery are important but not critical for inclusion in the strategy document. Similarly, the adoption of a control framework is not critical to having a successful information security strategy. Policies are developed subsequent to, and as a part of, implementing a strategy.

QUESTION 61
Which of the following is the BEST justification to convince management to invest in an information security program?

A. Cost reduction
B. Compliance with company policies
C. Protection of business assets
D. Increased business value
Real 51
Isaca CISM Exam

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 62
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

A. a statement regarding what the company will do with the information it collects.
B. a disclaimer regarding the accuracy of information on its web site.
C. technical information regarding how information is protected.
D. a statement regarding where the information is being hosted.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Most privacy laws and regulations require disclosure on how information will be used. A disclaimer is not necessary since it does not refer to data privacy. Technical details regarding how information is protected are not mandatory to publish on the web site and in fact would not be desirable. It is not mandatory to say where information is being hosted.

QUESTION 63
Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 64
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To improve the governance framework and achieve a higher level of maturity, an organization needs to conduct continuous analysis, monitoring and feedback compared to the current state of maturity. Return on security investment (ROSD may show the performance result of the security-

Real 53
Isaca CISM Exam

related activities; however, the result is interpreted in terms of money and extends to multiple facets of security initiatives. Thus, it may not be an adequate option. Continuous risk reduction would demonstrate the effectiveness of the security governance framework, but does not indicate a higher level of maturity. Key risk indicator (KRD setup is a tool to be used in internal control assessment. KRI setup presents a threshold to alert management when controls are being compromised in business processes. This is a control tool rather than a maturity model support tool.

QUESTION 65
Which of the following is MOST important to understand when developing a meaningful information security strategy?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Alignment of security with business objectives requires an understanding of what an organization is trying to accomplish. The other choices are all elements that must be considered, but their

Real 54
Isaca CISM Exam

importance is secondary and will vary depending on organizational goals.

QUESTION 66
Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness.
B. It is easier to manage and control.
C. It is more responsive to business unit needs.
D. It provides a faster turnaround for security requests.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 67
The FIRST step in establishing a security governance program is to:

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

Correct Answer: D
Section: (none)
Explanation

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

Real 56
Isaca CISM Exam

QUESTION 68
An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees Hood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example
of:

A. conflicting security controls with organizational needs.
B. strong protection of information resources.
C. implementing appropriate controls to reduce risk.
D. proving information security's protective abilities.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 69
Which of the following should be included in an annual information security budget that is submitted for management approval?

A. A cost-benefit analysis of budgeted resources
B. All of the resources that are recommended by the business
C. Total cost of ownership (TC'O)
D. Baseline comparisons

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
A brief explanation of the benefit of expenditures in the budget helps to convey the context of how the purchases that are being requested meet goals and objectives, which in turn helps build credibility for the information security function or program. Explanations of benefits also help engage senior management in the support of the information security program. While the budget should consider all inputs and recommendations that are received from the business, the budget that is ultimately submitted to management for approval should include only those elements that are intended for purchase. TC'O may be requested by management and may be provided in an addendum to a given purchase request, but is not usually included in an annual budget. Baseline comparisons (cost comparisons with other companies or industries) may be useful in developing a budget or providing justification in an internal review for an individual purchase, but would not be included with a request for budget approval.

QUESTION 70
Investment in security technology and processes should be based on:

A. clear alignment with the goals and objectives of the organization.
B. success cases that have been experienced in previous projects.
C. best business practices.
D. safeguards that are inherent in existing technology.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 71
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. analyzed under the retention policy.
B. protected under the information classification policy.
C. analyzed under the backup policy.
D. protected under the business impact analysis (BIA).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Option A is the type of analysis that will determine whether the organization is required to maintain the data for business, legal or regulatory reasons. Keeping data that are no longer required unnecessarily consumes resources, and, in the case of sensitive personal information, can increase the risk of data compromise. Options B. C and D are attributes that should be considered in the destruction and retention policy. A BIA could help determine that this information does not support the main objective of the business, but does not indicate the action to take.

QUESTION 72
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A company is held to the local laws and regulations of the country in which the company resides, even if the company decides to place servers with a vendor that hosts the servers in a foreign country. A potential violation of local laws applicable to the company might not be recognized or rectified (i.e., prosecuted) due to the lack of knowledge of the local laws that are applicable and the inability to enforce the laws. Option B is not a problem. Time difference does not play a role in a 24/7 environment. Pagers, cellular phones, telephones, etc. are usually available to communicate notifications. Option C is a manageable problem that requires additional funding, but

can be addressed. Option D is a problem that can be addressed. Most hosting providers have standardized the level of physical security that is in place. Regular physical audits or a SAS 70 report can address such concerns.

QUESTION 73
Effective IT governance is BEST ensured by:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 74
When an organization is implementing an information security governance program, its board of directors should be responsible for:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Real 62
Isaca CISM Exam

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.

QUESTION 75
Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 63
Isaca CISM Exam

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

QUESTION 76
An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 77
What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Real 65
Isaca CISM Exam

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.

QUESTION 78
The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

A. the plan aligns with the organization's business plan.
B. departmental budgets are allocated appropriately to pay for the plan.
C. regulatory oversight requirements are met.
D. the impact of the plan on the business units is reduced.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The steering committee controls the execution of the information security strategy according to the needs of the organization and decides on the project prioritization and the execution plan. The steering committee does not allocate department budgets for business units. While ensuring that regulatory oversight requirements are met could be a consideration, it is not the main reason for the review. Reducing the impact on the business units is a secondary concern but not the main reason for the review.

QUESTION 79
Which of the following is the BEST reason to perform a business impact analysis (BIA)?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The BIA is included as part of the process to determine the current state of risk and helps determine the acceptable levels of response from impacts and the current level of response, leading to a gap analysis. Budgeting appropriately may come as a result, but is not the reason to perform the analysis. Performing an analysis may satisfy regulatory requirements, bill is not the

Real 67
Isaca CISM Exam

reason to perform one. Analyzing the effect on the business is part of the process, but one must also determine the needs or acceptable effect or response.

Topic 2, INFORMATION RISK MANAGEMENT

QUESTION 80
A risk management program should reduce risk to:

A. zero.
B. an acceptable level.
C. an acceptable percent of revenue.
D. an acceptable probability of occurrence.

Correct Answer: B
Section: (none)
Explanation

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

Real 68
Isaca CISM Exam

probability of the risk.

QUESTION 81
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precise.
B. security risks are subject to frequent change.
C. reviewers can optimize and reduce the cost of controls.
D. it demonstrates to senior management that the security function can add value.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

QUESTION 82
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results

D. Amount of IT budget available

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 83
Which of the following will BEST protect an organization from internal security attacks?

Real 70
Isaca CISM Exam

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employee awareness certification program

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Because past performance is a strong predictor of future performance, background checks of prospective employees best prevents attacks from originating within an organization. Static IP addressing does little to prevent an internal attack. Internal address translation using non-routable addresses is useful against external attacks but not against internal attacks. Employees who certify that they have read security policies are desirable, but this does not guarantee that the employees behave honestly.

QUESTION 84
For risk management purposes, the value of an asset should be based on:

A. original cost.
B. net cash flow.
C. net present value.
D. replacement cost.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

QUESTION 85
Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.
C. control risk is minimized.

D. inherent risk is minimized.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 86
The MOST effective way to incorporate risk management practices into existing production systems is through:

A. policy development.
B. change management.
C. awareness training.
D. regular monitoring.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 73
Isaca CISM Exam

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

QUESTION 87
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 88
Risk acceptance is a component of which of the following?

A. Assessment

B. Mitigation
C. Evaluation
D. Monitoring

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 89
Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.
B. the point at which the benefit exceeds the expense.
C. a level that the organization is willing to accept.
D. a rate of return that equals the current cost of capital.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 90
A risk assessment should be conducted:

Real 76
Isaca CISM Exam

A. once a year for each business process and subprocess.
B. every three to six months for critical business processes.
C. by external parties to maintain objectivity.
D. annually or whenever there is a significant change.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 91
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

A. Theft of purchased software

B. Power outage lasting 24 hours
Real 77
Isaca CISM Exam
C. Permanent decline in customer confidence
D. Temporary loss of e-mail due to a virus attack

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 92
In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

A. original cost to acquire.
B. cost of the software stored.
C. annualized loss expectancy (ALE).
D. cost to obtain a replacement.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 78
Isaca CISM Exam

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

QUESTION 93
When residual risk is minimized:

A. acceptable risk is probable.
B. transferred risk is acceptable.
C. control risk is reduced.
D. risk is transferable.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

Real 79
Isaca CISM Exam

QUESTION 94
Quantitative risk analysis is MOST appropriate when assessment data:

A. include customer perceptions.
B. contain percentage estimates.
C. do not contain specific details.
D. contain subjective information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

QUESTION 95
Identification and prioritization of business risk enables project managers to:

A. establish implementation milestones.
Real 80
Isaca CISM Exam
B. reduce the overall amount of slack time.
C. address areas with most significance.
D. accelerate completion of critical paths.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 96
A risk analysis should:

A. include a benchmark of similar companies in its scope.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.
D. give more weight to the likelihood vs. the size of the loss.

Correct Answer: C
Section: (none)
Explanation

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 81
Isaca CISM Exam

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.

QUESTION 98
Which of the following BEST describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Risk analysis should include all organizational activities. It should not be limited to subsets of

Real 82
Isaca CISM Exam

systems or just systems and infrastructure.

QUESTION 99
The decision as to whether a risk has been reduced to an acceptable level should be determined by:

A. organizational requirements.
B. information systems requirements.
C. information security requirements.
D. international standards.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Organizational requirements should determine when a risk has been reduced to an acceptable level. Information systems and information security should not make the ultimate determination. Since each organization is unique, international standards of best practice do not represent the best solution.

QUESTION 100
Which of the following is the PRIMARY reason for implementing a risk management program?

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

Correct Answer: B
Section: (none)
Explanation

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

Real 83
Isaca CISM Exam

QUESTION 101
A successful risk management program should lead to:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 102
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

Real 84
Isaca CISM Exam

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 103
The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

A. hourly billing rate charged by the carrier.
B. value of the data transmitted over the network.
C. aggregate compensation of all affected business users.
D. financial losses incurred by affected business units.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

QUESTION 104
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 105
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

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

Correct Answer: B
Section: (none)
Explanation

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

Real 86
Isaca CISM Exam

QUESTION 106

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 107
Real 87
Isaca CISM Exam
In assessing risk, it is MOST essential to:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 108
When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

A. the information security steering committee.
B. customers who may be impacted.
C. data owners who may be impacted.
D. regulatory- agencies overseeing privacy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

QUESTION 109
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 110
It is important to classify and determine relative sensitivity of assets to ensure that:

A. cost of protection is in proportion to sensitivity.
B. highly sensitive assets are protected.
C. cost of controls is minimized.
D. countermeasures are proportional to risk.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 89
Isaca CISM Exam

Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

QUESTION 111
An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

A. threat.
B. loss.
C. vulnerability.
D. probability.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 90
Isaca CISM Exam

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

QUESTION 112
When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 113
The valuation of IT assets should be performed by:

A. an IT security manager.
B. an independent security consultant.
C. the chief financial officer (CFO).
D. the information owner.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 114
The PRIMARY objective of a risk management program is to:

A. minimize inherent risk.
B. eliminate business risk.
C. implement effective controls.
D. minimize residual risk.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The goal of a risk management program is to ensure that residual risk remains within manageable levels. Management of risk does not always require the removal of inherent risk nor is this always possible. A possible benefit of good risk management is to reduce insurance premiums, but this is

Real 92
Isaca CISM Exam

not its primary intention. Effective controls are naturally a clear objective of a risk management program, but with the choices given, choice C is an incomplete answer.

QUESTION 115
After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 116
When performing an information risk analysis, an information security manager should FIRST:

A. establish the ownership of assets.
B. evaluate the risks to the assets.
C. take an asset inventory.
D. categorize the assets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Assets must be inventoried before any of the other choices can be performed.

Real 93
Isaca CISM Exam

QUESTION 117
The PRIMARY benefit of performing an information asset classification is to:

A. link security requirements to business objectives.
B. identify controls commensurate to risk.
C. define access rights.
D. establish ownership.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All choices are benefits of information classification. However, identifying controls that are proportional to the risk in all cases is the primary benefit of the process.

QUESTION 118
Which of the following attacks is BEST mitigated by utilizing strong passwords?

A. Man-in-the-middle attack
   Real 94
   Isaca CISM Exam
B. Brute force attack
C. Remote buffer overflow
D. Root kit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 119
Phishing is BEST mitigated by which of the following?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 120
A security risk assessment exercise should be repeated at regular intervals because:

A. business threats are constantly changing.
B. omissions in earlier assessments can be addressed.
C. repetitive assessments allow various methodologies.
D. they help raise awareness on security in the business.

Correct Answer: A
Section: (none)

Explanation

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

QUESTION 121
Which of the following steps in conducting a risk assessment should be performed FIRST?

A. Identity business assets
B. Identify business risks
C. Assess vulnerabilities
D. Evaluate key controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk

by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

QUESTION 122
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 plans.
B. regularly testing the intrusion detection system (IDS).
C. establishing mandatory training of all personnel.
D. periodically reviewing incident response procedures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 123
Which of the following would a security manager establish to determine the target for restoration of normal processing?

A. Recover)' time objective (RTO)
B. Maximum tolerable outage (MTO)

C. Recovery point objectives (RPOs)
D. Services delivery objectives (SDOs)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

QUESTION 124
A risk management program would be expected to:

A. remove all inherent risk.
B. maintain residual risk at an acceptable level.
C. implement preventive controls for every threat.
D. reduce control risk to zero.

Correct Answer: B
Section: (none)
Explanation

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

Real 98
Isaca CISM Exam

QUESTION 125
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Real 99
Isaca CISM Exam

QUESTION 126
A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

A. there are sufficient safeguards in place to prevent this risk from happening.
B. the needed countermeasure is too complicated to deploy.
C. the cost of countermeasure outweighs the value of the asset and potential loss.
D. The likelihood of the risk occurring is unknown.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

QUESTION 127
Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

A. Number of controls implemented
B. Percent of control objectives accomplished
C. Percent of compliance with the security policy
D. Reduction in the number of reported security incidents

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

Real 100
Isaca CISM Exam

QUESTION 128
The PRIMARY purpose of using risk analysis within a security program is to:

A. justify the security expenditure.
B. help businesses prioritize the assets to be protected.
C. inform executive management of residual risk value.
D. assess exposures and plan remediation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 129
Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

Real 101
Isaca CISM Exam

A. Defining job roles
B. Performing a risk assessment
C. Identifying data owners
D. Establishing data retention policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Identifying the data owners is the first step, and is essential to implementing data classification. Defining job roles is not relevant. Performing a risk assessment is important, but will require the participation of data owners (who must first be identified). Establishing data retention policies may occur after data have been classified.

QUESTION 130
An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 131
A common concern with poorly written web applications is that they can allow an attacker to:

A. gain control through a buffer overflow.
B. conduct a distributed denial of service (DoS) attack.
C. abuse a race condition.
D. inject structured query language (SQL) statements.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Structured query language (SQL) injection is one of the most common and dangerous web application vulnerabilities. Buffer overflows and race conditions are very difficult to find and exploit on web applications.

Distributed denial of service (DoS) attacks have nothing to do with the quality of a web application.

QUESTION 132
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The security manager would be most concerned with whether residual risk would be reduced by a

greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

QUESTION 133
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 134
A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Creating a strong random password reduces the risk of a successful brute force attack by

Real 104
Isaca CISM Exam

exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

QUESTION 135
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 136
Which of the following would BEST address the risk of data leakage?

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

Correct Answer: C
Section: (none)
Explanation

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

Real 105
Isaca CISM Exam

QUESTION 137
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Real 106
Isaca CISM Exam

QUESTION 138
A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

A. A penetration test
B. A security baseline review
C. A risk assessment
D. A business impact analysis (BIA)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A risk assessment will identify- the business impact of such vulnerability being exploited and is, thus, the correct process. A penetration test or a security baseline review may identify the vulnerability but not the remedy. A business impact analysis (BIA) will more likely identify the impact of the loss of the mail server.

QUESTION 139
Which of the following measures would be MOST effective against insider threats to confidential information?

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

Correct Answer: A
Section: (none)
Explanation

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

Real 107
Isaca CISM Exam

QUESTION 140
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 141
Real 108
Isaca CISM Exam
The criticality and sensitivity of information assets is determined on the basis of:

A. threat assessment.
B. vulnerability assessment.
C. resource dependency assessment.
D. impact assessment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

QUESTION 142
When performing a risk assessment, the MOST important consideration is that:

A. management supports risk mitigation efforts.
   Real 109
   Isaca CISM Exam
B. annual loss expectations (ALEs) have been calculated for critical assets.
C. assets have been identified and appropriately valued.
D. attack motives, means and opportunities be understood.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. ALE calculations are only valid if assets have first been identified and appropriately valued. Motives, means and opportunities should already be factored

in as a part of a risk assessment.

QUESTION 143
The MAIN reason why asset classification is important to a successful information security program is because classification determines:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 144
The BEST strategy for risk management is to:

A. achieve a balance between risk and organizational goals.
B. reduce risk to an acceptable level.
C. ensure that policy development properly considers organizational risks.
D. ensure that all unmitigated risks are accepted by management.
Real 110
Isaca CISM Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to l>e considered a strategy.

QUESTION 145
An organization has to comply with recently published industry regulatory requirements--compliance that potentially has high implementation costs. What should the information security manager do FIRST?

A. Implement a security committee.
Real 111
Isaca CISM Exam
B. Perform a gap analysis.
C. Implement compensating controls.
D. Demand immediate compliance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 146
Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 147
One way to determine control effectiveness is by determining:

A. whether it is preventive, detective or compensatory.
B. the capability of providing notification of failure.
C. the test results of intended objectives.
D. the evaluation and analysis of reliability.
Real 112
Isaca CISM Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

QUESTION 148
What does a network vulnerability assessment intend to identify?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 149
After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

A. transferred.
B. treated.
C. accepted.
D. terminated.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 150
When a significant security breach occurs, what should be reported FIRST to senior management?

A. A summary of the security logs that illustrates the sequence of events
B. An explanation of the incident and corrective action taken
C. An analysis of the impact of similar attacks at other organizations
D. A business case for implementing stronger logical access controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When reporting an incident to senior management, the initial information to be communicated should include an explanation of what happened and how the breach was resolved. A summary of security logs would be too technical to report to senior management. An analysis of the impact of similar attacks and a business case for improving controls would be desirable; however, these

would be communicated later in the process.

QUESTION 151
The PRIMARY reason for initiating a policy exception process is when:

A. operations are too busy to comply.
B. the risk is justified by the benefit.
C. policy compliance would be difficult to enforce.
D. users may initially be inconvenienced.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Exceptions to policy are warranted in circumstances where compliance may be difficult or impossible and the risk of noncompliance is outweighed by the benefits. Being busy is not a justification for policy exceptions, nor is the fact that compliance cannot be enforced. User inconvenience is not a reason to automatically grant exception to a policy.

QUESTION 152
Which of (lie following would be the MOST relevant factor when defining the information classification policy?

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

Correct Answer: D
Section: (none)
Explanation

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

Real 115
Isaca CISM Exam

QUESTION 153
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 department.
B. database administrator.
C. chief information officer (CIO).
D. head of the sales department.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 154
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

Real 116
Isaca CISM Exam

A. develop an operational plan for achieving compliance with the legislation.
B. identify systems and processes that contain privacy components.
C. restrict the collection of personal information until compliant.

D. identify privacy legislation in other countries that may contain similar requirements.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 155
Risk assessment is MOST effective when performed:

A. at the beginning of security program development.
B. on a continuous basis.
C. while developing the business case for the security program.
D. during the business change process.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 156
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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 157
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

A. Countermeasure cost-benefit analysis
B. Penetration testing
C. Frequent risk assessment programs

D. Annual loss expectancy (ALE) calculation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control. Frequent risk assessment programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will contribute to the value of the risk but. alone, will not justify a control.

QUESTION 158
An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance

Real 119
Isaca CISM Exam

so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

QUESTION 159
Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 160

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The assigned class of sensitivity and criticality of the information resource determines the level of access controls to be put in place. The assignment of sensitivity and criticality takes place with the information assets that have already been included in the information security program and has

only an indirect bearing on the costs to be incurred. The assignment of sensitivity and criticality contributes to, but does not decide, the overall budget of the information security program.

QUESTION 161
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 162
Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Effective risk management requires participation, support and acceptance by all applicable members of the

organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

QUESTION 163
The MOST effective use of a risk register is to:

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

Correct Answer: C
Section: (none)
Explanation

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

Real 122
Isaca CISM Exam

QUESTION 164
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 165
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 166
A risk management approach to information protection is:

Real 123
Isaca CISM Exam

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 167
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

Real 124
Isaca CISM Exam
continuity planning?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 168
An information security organization should PRIMARILY:

A. support the business objectives of the company by providing security-related support services.
B. be responsible for setting up and documenting the information security responsibilities of the information security team members.
C. ensure that the information security policies of the company are in line with global best practices and standards.

D. ensure that the information security expectations are conveyed to employees.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 169
All risk management activities are PRIMARILY designed to reduce impacts to:

A. a level defined by the security manager.
B. an acceptable level based on organizational risk tolerance.
C. a minimum level consistent with regulatory requirements.
D. the minimum level possible.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The aim of risk management is to reduce impacts to an acceptable level. "Acceptable" or "reasonable" are relative terms that can vary based on environment and circumstances. A minimum level that is consistent with regulatory requirements may not be consistent with business objectives, and regulators typically do not assign risk levels. The minimum level possible may not be aligned with business requirements.

QUESTION 170
After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

A. Information security officer
   Real 126
   Isaca CISM Exam
B. Chief information officer (CIO)
C. Business owner
D. Chief executive officer (CF.O)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The business owner of the application needs to understand and accept the residual application risks.

QUESTION 171
Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

A. Performing a business impact analysis (BIA)
B. Considering personal information devices as pan of the security policy
C. Initiating IT security training and familiarization
D. Basing the information security infrastructure on risk assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The information security infrastructure should be based on risk. While considering personal

information devices as part of the security policy may be a consideration, it is not the most important requirement. A BIA is typically carried out to prioritize business processes as part of a business continuity plan. Initiating IT security training may not be important for the purpose of the information security infrastructure.

QUESTION 172
Previously accepted risk should be:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 173
Which of the following steps should be performed FIRST in the risk assessment process?

A. Staff interviews
B. Threat identification
C. Asset identification and valuation
D. Determination of the likelihood of identified risks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk. Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

QUESTION 174
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism
C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Real 129
Isaca CISM Exam

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

QUESTION 175
Who can BEST advocate the development of and ensure the success of an information security program?

Real 130
Isaca CISM Exam

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 176
The effectiveness of virus detection software is MOST dependent on which of the following?

A. Packet filtering
B. Intrusion detection
C. Software upgrades
D. D. Definition tables
Real 131
Isaca CISM Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 177
Which of the following is the MOST effective type of access control?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 178
An intrusion detection system should be placed:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical dcvice.

QUESTION 179
The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

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

Correct Answer: C
Section: (none)
Explanation

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

Real 133
Isaca CISM Exam

QUESTION 180
An extranet server should be placed:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 181
Which of the following is the BEST metric for evaluating the effectiveness of security awareness twining? The number of:

A. password resets.
B. reported incidents.
C. incidents resolved.
D. access rule violations.

Correct Answer: B
Section: (none)
Explanation

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

Real 134
Isaca CISM Exam

QUESTION 182
Security monitoring mechanisms should PRIMARILY:

A. focus on business-critical information.
B. assist owners to manage control risks.
C. focus on detecting network intrusions.
D. record all security violations.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security monitoring must focus on business-critical information to remain effectively usable by and credible

to business users. Control risk is the possibility that controls would not detect an incident or error condition, and therefore is not a correct answer because monitoring would not directly assist in managing this risk. Network intrusions are not the only focus of monitoring mechanisms; although they should record all security violations, this is not the primary objective.

QUESTION 183
When contracting with an outsourcer to provide security administration, the MOST important

Real 135
Isaca CISM Exam
contractual element is the:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 184
Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 185
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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 186
Which of the following is MOST effective in preventing security weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Configuration management
Real 137
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 187
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 188
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 189
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Real 139
Isaca CISM Exam

other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

QUESTION 190
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Real 140
Isaca CISM Exam

QUESTION 191
On which of the following should a firewall be placed?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 192
Access control to a sensitive intranet application by mobile users can BEST be implemented through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 193
When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 194
The information classification scheme should:

A. consider possible impact of a security breach.
B. classify personal information in electronic form.
C. be performed by the information security manager.
D. classify systems according to the data processed.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
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.

QUESTION 195
An information security program should be sponsored by:

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

Correct Answer: C
Section: (none)
Explanation

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

Real 144
Isaca CISM Exam

QUESTION 196
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 197
The BEST metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocked.
B. number of packets dropped.
C. average throughput rate.
D. number of firewall rules.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 198
The MAIN advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workload.
B. increases security between multi-tier systems.
C. allows passwords to be changed less frequently.
D. reduces the need for two-factor authentication.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 199
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 200
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 201
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

A. Rewrite the application to conform to the upgraded operating system
B. Compensate for not installing the patch with mitigating controls
C. Alter the patch to allow the application to run in a privileged state
D. Run the application on a test platform; tune production to allow patch and application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 147
Isaca CISM Exam

Since the operating system (OS) patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security . Since the application is critical, the patch should not be applied without regard for the application; business requirements must be considered. Altering the OS patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative since it will mean running a critical production application on a platform not subject to the same level of security controls.

QUESTION 202
Which of the following is MOST important for a successful information security program?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sufficient executive management support is the most important factor for the success of an information security program. Open communication, adequate training, and good policies and

Real 148
Isaca CISM Exam

procedures, while important, are not as important as support from top management; they will not ensure success if senior management support is not present.

QUESTION 203
Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 204
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 205
Which of the following devices should be placed within a DMZ?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Real 150
Isaca CISM Exam

QUESTION 206
A border router should be placed on which of the following?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 207
Real 151
Isaca CISM Exam
Secure customer use of an e-commerce application can BEST be accomplished through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 208
Real 152
Isaca CISM Exam
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

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

Correct Answer: A
Section: (none)

Explanation

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

QUESTION 209
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 210
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
   Real 153
   Isaca CISM Exam
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 211
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Real 154
Isaca CISM Exam

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

QUESTION 212
Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 213
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software

Real 155
Isaca CISM Exam

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

QUESTION 214
The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

A. helps ensure that communications are secure.
B. increases security between multi-tier systems.
C. allows passwords to be changed less frequently.

D. eliminates the need for secondary authentication.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 215
Which of the following is MOST effective in protecting against the attack technique known as phishing?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 216
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 217
Which of the following is the MOST important risk associated with middleware in a client-server environment?

Real 157
Isaca CISM Exam

A. Server patching may be prevented
B. System backups may be incomplete
C. System integrity may be affected
D. End-user sessions may be hijacked

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely to occur.

QUESTION 218
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

Real 158
Isaca CISM Exam

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 219
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 220
An information security manager uses security metrics to measure the:

A. performance of the information security program.

B. performance of the security baseline.
C. effectiveness of the security risk analysis.
D. effectiveness of the incident response team.

Correct Answer: A
Section: (none)
Explanation

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

Real 160
Isaca CISM Exam

QUESTION 221
Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

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

Correct Answer: B
Section: (none)
Explanation

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

Real 161
Isaca CISM Exam

QUESTION 222
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Web browsers have the capability of authenticating through client-based certificates; nevertheless, it is not commonly used. When using https, servers always authenticate with a certificate and, once the connection

is established, confidentiality will be maintained between client and server. By default, web browsers and servers support multiple encryption algorithms and negotiate the best option upon connection.

QUESTION 223
The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

A. Secure Sockets Layer (SSL).
B. Secure Shell (SSH).
C. IP Security (IPSec).
D. Secure/Multipurpose Internet Mail Extensions (S/MIME).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet. In typical use, all data transmitted between the customer and the business are, therefore, encrypted by the business's web server and remain confidential. SSH File Transfer Protocol (SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with the SSH-2 protocol to provide secure file transfer. IP Security (IPSec) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPSec operation: transport mode and tunnel mode. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of e-mail encapsulated in MIME; it is not a web transaction

Real 162
Isaca CISM Exam

protocol.

QUESTION 224
A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:

A. authentication and authorization.
B. confidentiality and integrity.
C. confidentiality and nonrepudiation.
D. authentication and nonrepudiation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Encryption by the private key of the sender will guarantee authentication and nonrepudiation. Encryption by the public key of the receiver will guarantee confidentiality.

QUESTION 225
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

A. Security compliant servers trend report
B. Percentage of security compliant servers
C. Number of security patches applied
D. Security patches applied trend report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The percentage of compliant servers will be a relevant indicator of the risk exposure of the infrastructure. However, the percentage is less relevant than the overall trend, which would provide a measurement of the efficiency of the IT security program. The number of patches applied would be less relevant, as this would depend on the number of vulnerabilities identified and patches provided by vendors.

QUESTION 226
It is important to develop an information security baseline because it helps to define:

A. critical information resources needing protection.
B. a security policy for the entire organization.
C. the minimum acceptable security to be implemented.
D. required physical and logical access controls.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 227
Which of the following BEST provides message integrity, sender identity authentication and

Real 164
Isaca CISM Exam
nonrepudiation?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 228
To BEST improve the alignment of the information security objectives in an organization, the chief

Real 165
Isaca CISM Exam
information security officer (CISO) should:

A. revise the information security program.
B. evaluate a balanced business scorecard.
C. conduct regular user awareness sessions.
D. perform penetration tests.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 229
What is the MOST important item to be included in an information security policy?

A. The definition of roles and responsibilities
B. The scope of the security program
C. The key objectives of the security program
D. Reference to procedures and standards of the security program

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 230
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. invite an external consultant to create the security strategy.
B. allocate budget based on best practices.
C. benchmark similar organizations.
D. define high-level business security requirements.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 231
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

A. Number of controls

B. Cost of achieving control objectives
C. Effectiveness of controls
D. Test results of controls
Real 167
Isaca CISM Exam

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 232
Which of the following is a key area of the ISO 27001 framework?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 168
Isaca CISM Exam

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

QUESTION 233
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 234
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the system.
B. implement multifactor authentication.
C. rebuild the system from the original installation medium.
D. disconnect the mail server from the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

QUESTION 235
The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

A. verify the decision with the business units.
B. check the system's risk analysis.
C. recommend update after post implementation review.
D. request an audit review.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Verifying the decision with the business units is the correct answer because it is not the IT function's responsibility to decide whether a new application modifies business processes Choice B does not consider the change in the applications. Choices C and D delay the update.

QUESTION 236
The PRIMARY objective of an Internet usage policy is to prevent:

A. access to inappropriate sites.
B. downloading malicious code.
C. violation of copyright laws.
D. disruption of Internet access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Unavailability of Internet access would cause a business disruption. The other three objectives are secondary.

Real 171
Isaca CISM Exam

QUESTION 237
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 authentication.
B. unvalidated input.
C. cross-site scripting.
D. structured query language (SQL) injection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 238
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Real 172
Isaca CISM Exam

QUESTION 239
In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

A. a strong authentication.
B. IP antispoofing filtering.
C. network encryption protocol.
D. access lists of trusted devices.

Correct Answer: A
Section: (none)
Explanation

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

Real 173
Isaca CISM Exam

QUESTION 240
Priority should be given to which of the following to ensure effective implementation of information security governance?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 241
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 242
Which of the following is the MOST important reason why information security objectives should be defined?

A. Tool for measuring effectiveness
B. General understanding of goals
C. Consistency with applicable standards
D. Management sign-off and support initiatives
Real 175
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 243
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 program.
B. recruitment of technical IT employees.
C. periodic risk assessments.
D. security awareness training for employees.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

Real 176
Isaca CISM Exam

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.

QUESTION 244
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 245
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 246
At what stage of the applications development process would encryption key management initially be addressed?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 247
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 248
A digital signature using a public key infrastructure (PKI) will:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The certificate authority (CA) is a trusted third party that attests to the identity of the signatory, and

Real 179
Isaca CISM Exam

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.

QUESTION 249
Which of the following is the BEST method to securely transfer a message?

A. Password-protected removable media
B. Facsimile transmission in a secured room
C. Using public key infrastructure (PKI) encryption
D. Steganography
Real 180
Isaca CISM Exam

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 250
Which of the following would be the FIRST step in establishing an information security program?

A. Develop the security policy.
B. Develop security operating procedures.
C. Develop the security plan.
D. Conduct a security controls study.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security plan must be developed to implement the security strategy. All of the other choices should follow the development of the security plan.

QUESTION 251
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

A. the parties to the agreement can perform.
B. confidential data are not included in the agreement.
C. appropriate controls are included.
D. the right to audit is a requirement.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 252
For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a

typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

QUESTION 253

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Real 183
Isaca CISM Exam

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.

QUESTION 254
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 255
Nonrepudiation can BEST be ensured by using:

A. strong passwords.
B. a digital hash.
C. symmetric encryption.
D. digital signatures.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Real 184
Isaca CISM Exam

Topic 4, INFORMATION SECURITY PROGRAM MANAGEMENT

QUESTION 256
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testing.
B. establish security baselines.
C. implement vendor default settings.
D. link policies to an independent standard.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 257
The BEST way to ensure that information security policies are followed is to:

A. distribute printed copies to all employees.
B. perform periodic reviews for compliance.
C. include escalating penalties for noncompliance.
D. establish an anonymous hotline to report policy abuses.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 258
The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

A. system developer.
B. information security manager.
C. steering committee.
D. system data owner.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data owners are the most knowledgeable of the security needs of the business application for which they are responsible. The system developer, security manager and system custodian will have specific knowledge on limited areas but will not have full knowledge of the business issues that affect the level of security required. The steering committee does not perform at that level of detail on the operation.

Real 186
Isaca CISM Exam

QUESTION 259
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 260
The BEST way to ensure that an external service provider complies with organizational security

Real 187
Isaca CISM Exam
policies is to:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 261
When an emergency security patch is received via electronic mail, the patch should FIRST be:

A. loaded onto an isolated test machine.
B. decompiled to check for malicious code.
C. validated to ensure its authenticity.
D. copied onto write-once media to prevent tampering.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 262
Which of the following is the BEST indicator that security awareness training has been effective?

A. Employees sign to acknowledge the security policy
B. More incidents are being reported
C. A majority of employees have completed training
D. No incidents have been reported in three months

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
More incidents being reported could be an indicator that the staff is paying more attention to security. Employee signatures and training completion may or may not have anything to do with awareness levels. The number of individuals trained may not indicate they are more aware. No recent security incidents does not reflect awareness levels, but may prompt further research to confirm.

QUESTION 263
Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs?

A. Penetration attempts investigated
B. Violation log reports produced
C. Violation log entries
D. Frequency of corrective actions taken

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The most useful metric is one that measures the degree to which complete follow-through has

taken place. The quantity of reports, entries on reports and the frequency of corrective actions are not indicative of whether or not investigative action was taken.

QUESTION 264
Which of the following is the MOST important management signoff for migrating an order processing system from a test environment to a production environment?

A. User
B. Security
C. Operations
D. Database

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
As owners of the system, user management approval would be the most important. Although the signoffs of security, operations and database management may be appropriate, they are secondary to ensuring the new system meets the requirements of the business.

Real 190
Isaca CISM Exam

QUESTION 265
Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

A. the third party provides a demonstration on a test system.
B. goals and objectives are clearly defined.
C. the technical staff has been briefed on what to expect.
D. special backups of production servers are taken.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 266
Real 191
Isaca CISM Exam
Which of the following is MOST important to the successful promotion of good security management practices?

A. Security metrics
B. Security baselines
C. Management support
D. Periodic training

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Without management support, all other efforts will be undermined. Metrics, baselines and training are all important, but they depend on management support for their success.

QUESTION 267
Which of the following environments represents the GREATEST risk to organizational security?

A. Locally managed file server
B. Enterprise data warehouse
C. Load-balanced, web server cluster
D. Centrally managed data switch

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
A locally managed file server will be the least likely to conform to organizational security policies because it is generally subject to less oversight and monitoring. Centrally managed data switches, web server clusters and data warehouses are subject to close scrutiny, good change control practices and monitoring.

QUESTION 268
Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 269
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 193
Isaca CISM Exam

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.

QUESTION 270
Security policies should be aligned MOST closely with:

A. industry' best practices.
B. organizational needs.
C. generally accepted standards.
D. local laws and regulations.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 271
The BEST time to perform a penetration test is after:

A. an attempted penetration has occurred.
B. an audit has reported weaknesses in security controls.
C. various infrastructure changes are made.
D. a high turnover in systems staff.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Changes in the systems infrastructure are most likely to inadvertently introduce new exposures. Conducting a test after an attempted penetration is not as productive since an organization should not wait until it is attacked to test its defenses. Any exposure identified by an audit should be corrected before it would be appropriate to test. A turnover in administrative staff does not warrant a penetration test, although it may-warrant a review of password change practices and configuration management.

QUESTION 272
Successful social engineering attacks can BEST be prevented through:

A. preemployment screening.
B. close monitoring of users' access patterns.
C. periodic awareness training.
D. efficient termination procedures.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 273
Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The fact that operating system (OS) security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user ad hoc

reporting is not necessarily good, it does not represent as serious a security- weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

QUESTION 274
In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

A. Implementing on-screen masking of passwords
   Real 196
   Isaca CISM Exam
B. Conducting periodic security awareness programs
C. Increasing the frequency of password changes
D. Requiring that passwords be kept strictly confidential

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt. Implementing on-screen masking of passwords and increasing the frequency of password changes are desirable, but these will not be effective in reducing the likelihood of a successful social engineering attack. Requiring that passwords be kept secret in security policies is a good control but is not as effective as periodic security awareness programs that will alert users of the dangers posed by social engineering.

QUESTION 275
Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security- steering committees
D. Security awareness campaigns

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self-assessment exercises are all good but do not exemplify the taking of ownership by management.

QUESTION 276
What is the BEST way to ensure that contract programmers comply with organizational security policies?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Periodic reviews are the most effective way of obtaining compliance. None of the other options detects the

failure of contract programmers to comply.

QUESTION 277
Which of the following activities is MOST likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 198
Isaca CISM Exam

If malicious code is not immediately detected, it will most likely be backed up as a part of the normal tape backup process. When later discovered, the code may be eradicated from the device but still remain undetected ON a backup tape. Any subsequent restores using that tape may reintroduce the malicious code. Applying patches, changing access rules and upgrading hardware does not significantly increase the level of difficulty.

QUESTION 278
What is the BEST method to verify that all security patches applied to servers were properly documented?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To ensure that all patches applied went through the change control process, it is necessary to use the operating system (OS) patch logs as a starting point and then check to see if change control documents are on file for each of these changes. Tracing from the documentation to the patch log

Real 199
Isaca CISM Exam

will not indicate if some patches were applied without being documented. Similarly, reviewing change control documents for key servers or comparing patches applied to those recommended by the OS vendor's web site does not confirm that these security patches were properly approved and documented.

QUESTION 279
A security awareness program should:

A. present top management's perspective.
B. address details on specific exploits.
C. address specific groups and roles.
D. promote security department procedures.

Correct Answer: C

Section: (none)
Explanation

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

QUESTION 280
The PRIMARY objective of security awareness is to:

A. ensure that security policies are understood.
B. influence employee behavior.
C. ensure legal and regulatory compliance
D. notify of actions for noncompliance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Real 200
Isaca CISM Exam

QUESTION 281
Which of the following will BEST protect against malicious activity by a former employee?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 282
The return on investment of information security can BEST be evaluated through which of the following?

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

Correct Answer: A

Section: (none)
Explanation

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

QUESTION 283
To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

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

Correct Answer: B
Section: (none)
Explanation

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

Real 202
Isaca CISM Exam

QUESTION 284
Information security policies should:

A. address corporate network vulnerabilities.
B. address the process for communicating a violation.
C. be straightforward and easy to understand.
D. be customized to specific groups and roles.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As high-level statements, information security policies should be straightforward and easy to understand. They arc high-level and, therefore, do not address network vulnerabilities directly or the process for communicating a violation. As policies, they should provide a uniform message to all groups and user roles.

QUESTION 285
Real 203
Isaca CISM Exam
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 286
Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 287
Security audit reviews should PRIMARILY:

A. ensure that controls operate as required.
B. ensure that controls are cost-effective.
C. focus on preventive controls.
D. ensure controls are technologically current.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The primary objective of a security review or audit should be to provide assurance on the adequacy of security controls. Reviews should focus on all forms of control, not just on preventive control. Cost-effectiveness and technological currency are important but not as critical.

QUESTION 288
Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into

Real 205
Isaca CISM Exam

two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting ;in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

QUESTION 289
Which of the following is an inherent weakness of signature-based intrusion detection systems?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and

Real 206
Isaca CISM Exam

spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

QUESTION 290
Data owners are normally responsible for which of the following?

A. Applying emergency changes to application data
B. Administering security over database records
C. Migrating application code changes to production
D. Determining the level of application security required

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data owners approve access to data and determine the degree of protection that should be applied (data classification). Administering database security, making emergency changes to data and migrating code to production are infrastructure tasks performed by custodians of the data.

QUESTION 291
Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

A. System analyst
B. System user
C. Operations manager
D. Data security officer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
System users, specifically the user acceptance testers, would be in the best position to note whether new exposures are introduced during the change management process. The system designer or system analyst, data security officer and operations manager would not be as closely involved in testing code changes.

Real 207
Isaca CISM Exam

QUESTION 292
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 293
Which of the following would present the GREATEST risk to information security?

A. Virus signature files updates are applied to all servers every day
B. Security access logs are reviewed within five business days Real 208
Isaca CISM Exam
C. Critical patches are applied within 24 hours of their release
D. Security incidents are investigated within five business days

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security incidents are configured to capture system events that are important from the security perspective; they include incidents also captured in the security access logs and other monitoring tools. Although, in some instances, they could wait for a few days before they are researched, from the options given this would have the greatest risk to security. Most often, they should be analyzed as soon as possible. Virus signatures should be updated as often as they become available by the vendor, while critical patches should be installed as soon as they are reviewed and tested, which could occur in 24 hours.

QUESTION 294
The PRIMARY reason for using metrics to evaluate information security is to:

A. identify security weaknesses.
B. justify budgetary expenditures.
C. enable steady improvement.

D. raise awareness on security issues.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 295
What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodic review of network configuration
B. Review intrusion detection system (IDS) logs for evidence of attacks
C. Periodically perform penetration tests
D. Daily review of server logs for evidence of hacker activity Real 209
Isaca CISM Exam

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 296
Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used
B. Provide clear directions to IT staff
C. Monitor intrusion detection system (IDS) and firewall logs closely
D. Establish clear rules of engagement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It is critical to establish a clear understanding on what is permissible during the engagement.

Real 210
Isaca CISM Exam

Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used. As for monitoring the intrusion detection system (IDS) and firewall, and providing directions to IT staff, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

QUESTION 297
Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

A. Restrict the available drive allocation on all PCs
B. Disable universal serial bus (USB) ports on all desktop devices
C. Conduct frequent awareness training with noncompliance penalties
D. Establish strict access controls to sensitive information

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Restricting the ability of a PC to allocate new drive letters ensures that universal serial bus (USB) drives or even CD-writers cannot be attached as they would not be recognized by the operating system. Disabling USB ports on all machines is not practical since mice and other peripherals depend on these connections. Awareness training and sanctions do not prevent copying of information nor do access controls.

QUESTION 298
Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The number of individuals with access to the network configuration presents a security risk.

Real 211
Isaca CISM Exam

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

QUESTION 299
Good information security procedures should:

A. define the allowable limits of behavior.
B. underline the importance of security governance.
C. describe security baselines for each platform.
D. be updated frequently as new software is released.

Correct Answer: D
Section: (none)
Explanation

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

Real 212

Isaca CISM Exam

QUESTION 300
What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 301
A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

A. Sign a legal agreement assigning them all liability for any breach
B. Remove all trading partner access until the situation improves
C. Set up firewall rules restricting network traffic from that location
D. Send periodic reminders advising them of their noncompliance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It is incumbent on an information security manager to see to the protection of their organization's network, but to do so in a manner that does not adversely affect the conduct of business. This can be accomplished by adding specific traffic restrictions for that particular location. Removing all access will likely result in lost business. Agreements and reminders do not protect the integrity of the network.

Real 213
Isaca CISM Exam

QUESTION 302
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 303
What is the MOST appropriate change management procedure for the handling of emergency

Real 214
Isaca CISM Exam
program changes?

A. Formal documentation does not need to be completed before the change
B. Business management approval must be obtained prior to the change
C. Documentation is completed with approval soon after the change
D. All changes must follow the same process

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Even in the case of an emergency change, all change management procedure steps should be completed as in the case of normal changes. The difference lies in the timing of certain events. With an emergency change, it is permissible to obtain certain approvals and other documentation on "the morning after" once the emergency has been satisfactorily resolved. Obtaining business approval prior to the change is ideal but not always possible.

QUESTION 304
The PRIMARY focus of the change control process is to ensure that changes are:

A. authorized.
Real 215
Isaca CISM Exam
B. applied.
C. documented.
D. tested.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 305
An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

A. Research best practices
B. Meet with stakeholders
C. Establish change control procedures
D. Identify critical systems

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
No new process will be successful unless it is adhered to by all stakeholders; to the extent stakeholders

have input, they can be expected to follow the process. Without consensus agreement from the stakeholders, the scope of the research is too wide; input on the current environment is necessary to focus research effectively. It is premature to implement procedures without stakeholder consensus and research. Without knowing what the process will be the parameters to baseline are unknown as well.

QUESTION 306
Which of the following documents would be the BES T reference to determine whether access control mechanisms are appropriate for a critical application?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 307
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

A. The right to conduct independent security reviews
B. A legally binding data protection agreement
   Real 217
   Isaca CISM Exam
C. Encryption between the organization and the provider
D. A joint risk assessment of the system

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 308
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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
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.

QUESTION 309
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 only.
B. implement role-based access control in the application.
Real 218
Isaca CISM Exam
C. enforce manual procedures ensuring separation of conflicting duties.
D. create service accounts that can only be used by authorized team members.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 310
In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

Real 219
Isaca CISM Exam

A. testing time window prior to deployment.
B. technical skills of the team responsible.
C. certification of validity for deployment.
D. automated deployment to all the servers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Having the patch tested prior to implementation on critical systems is an absolute prerequisite where availability is a primary concern because deploying patches that could cause a system to fail could be worse than the vulnerability corrected by the patch. It makes no sense to deploy patches on every system. Vulnerable systems should be the only candidate for patching. Patching skills are not required since patches are more often applied via automated tools.

QUESTION 311
To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

A. end users.

B. legal counsel.
C. operational units.
D. audit management.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Procedures at the operational level must be developed by or with the involvement of operational units that will use them. This will ensure that they are functional and accurate. End users and legal counsel are normally not involved in procedure development. Audit management generally oversees information security operations but does not get involved at the procedural level.

QUESTION 312
When security policies are strictly enforced, the initial impact is that:

A. they may have to be modified more frequently.
B. they will be less subject to challenge.
C. the total cost of security is increased.
D. the need for compliance reviews is decreased.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 313
A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

A. an effective control over connectivity and continuity.
B. a service level agreement (SLA) including code escrow.
C. a business impact analysis (BIA).
D. a third-party certification.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The principal risk focus is the connection procedures to maintain continuity- in case of any

contingency. Although an information security manager may be interested in the service level agreement (SLA), code escrow is not a concern. A business impact analysis (BIA) refers to contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

QUESTION 314
What is the MOST important element to include when developing user security awareness material?

A. Information regarding social engineering
B. Detailed security policies
C. Senior management endorsement
D. Easy-to-read and compelling information

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Making security awareness material easy and compelling to read is the most important success factor. Users must be able to understand, in easy terms, complex security concepts in a way that makes compliance more accessible. Choice A would also be important but it needs to be

presented in an adequate format. Detailed security policies might not necessarily be included in the training materials. Senior management endorsement is important for the security program as a whole and not necessarily for the awareness training material.

QUESTION 315
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 316
The configuration management plan should PRIMARILY be based upon input from:

A. business process owners.
B. the information security manager.
C. the security steering committee.
D. IT senior management.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 317
Which of the following is the MOST effective, positive method to promote security awareness?

A. Competitions and rewards for compliance
B. Lock-out after three incorrect password attempts
C. Strict enforcement of password formats
D. Disciplinary action for noncompliance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

QUESTION 318
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 319
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop
Real 225
Isaca CISM Exam

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 320
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 226
Isaca CISM Exam

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.

QUESTION 322
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 323
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 324
Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security should be an integral component of the development cycle; thus, it should be

included at the process level. Choices A, B and C are good mechanisms to ensure compliance, but would not be nearly as timely in ensuring that the plans are always up-to-date. Choice D is a preventive control, while choices A, B and C are detective controls.

QUESTION 325
When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/disaster recovery plans is because:

A. this is a requirement of the security policy.
B. software licenses may expire in the future without warning.
C. the asset inventory must be maintained.
D. service level agreements may not otherwise be met.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
The key requirement is to preserve availability of business operations. Choice A is a correct compliance requirement, but is not the main objective in this case. Choices B and C are supplementary requirements for business continuity/disaster recovery planning.

QUESTION 326
To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOS T important item to include?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Service level agreements (QUESTION NO: As) will be most effective in ensuring that Internet service providers (ISPs) comply with expectations for service availability. Intrusion detection system (IDS) and spam filtering services would not mitigate (as directly) the potential for service

Real 229
Isaca CISM Exam

interruptions. A right-to-audit clause would not be effective in mitigating the likelihood of a service interruption.

QUESTION 327
Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

A. are compatible with the provider's own classification.
B. are communicated to the provider.
C. exceed those of the outsourcer.
D. are stated in the contract.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A. B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

Real 230
Isaca CISM Exam

QUESTION 328
What is the GREATEST risk when there is an excessive number of firewall rules?

A. One rule may override another rule in the chain and create a loophole
B. Performance degradation of the whole network
C. The firewall may not support the increasing number of rules due to limitations

D. The firewall may show abnormal behavior and may crash or automatically shut down

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If there are many firewall rules, there is a chance that a particular rule may allow an external connection although other associated rules are overridden. Due to the increasing number of rules, it becomes complex to test them and. over time, a loophole may occur.

QUESTION 329
Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

A. Mantrap
B. Biometric lock
C. Closed-circuit television (CCTV)
D. Security guard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

QUESTION 330
Real 231
Isaca CISM Exam
What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 331
What is the BEST way to ensure data protection upon termination of employment?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 332
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 333
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
Real 233
Isaca CISM Exam
C. Systems programmer
D. Security administrator

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 334
Which would be the BEST recommendation to protect against phishing attacks?

Real 234
Isaca CISM Exam

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 335
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 issues.
B. The cost of implementing a security control is less than the value of the assets.
C. The percentage of systems that is compliant with security standards.
D. The audit reports do not reflect any significant findings on security.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 336
What is the BEST way to alleviate security team understaffing while retaining the capability in- house?

A. Hire a contractor that would not be included in the permanent headcount
B. Outsource with a security services provider while retaining the control internally
C. Establish a virtual security team from competent employees across the company
D. Provide cross training to minimize the existing resources gap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While hiring an indirect resource that will not be part of headcount will help to add an extra

resource, it usually costs more than a direct employee; thus, it is not cost efficient. Outsourcing may be a more expensive option and can add complexities to the service delivery. Competent security staff can be recruited from other departments e.g., IT. product development, research and development (R&D). By leveraging existing resources, there is a nominal additional cost. It is also a strategic option since the staff may join the team as full members in the future (internal transfer). Development of staff is often a budget drain and, if not managed carefully, these resources may move away from the company and leave the team with a bigger resource gap.

QUESTION 337
Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

A. policy.

B. strategy.
C. guideline
D. baseline.
Real 236
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 338
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 organizations.
B. past experience of the engagement team.
C. sample deliverable.
D. methodology used in the assessment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 339
Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

A. assess the problems and institute rollback procedures, if needed.
B. disconnect the systems from the network until the problems are corrected.
C. immediately uninstall the patches from these systems.
D. immediately contact the vendor regarding the problems that occurred.
Real 237
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 340
When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by

a third-party service provider, the BEST indicator of compliance would be the:

A. access control matrix.
B. encryption strength.
C. authentication mechanism.
D. data repository.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 341
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 system.
B. sustaining the organization's security posture.
C. the existing systems that will be affected.
D. complying with segregation of duties.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Real 238
Isaca CISM Exam

primary reason to involve security in the systems development life cycle (SDLC).

QUESTION 342
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 343
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 239
Isaca CISM Exam

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

QUESTION 344
An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

A. source routing.
B. broadcast propagation.
C. unregistered ports.
D. nonstandard protocols.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 345
What is the MOS T cost-effective means of improving security awareness of staff personnel?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
User education and training is the most cost-effective means of influencing staff to improve security since personnel are the weakest link in security. Incentives perform poorly without user education and training. A zero-tolerance security policy would not be as good as education and

Real 240
Isaca CISM Exam

training. Users would not have the knowledge to accurately interpret and report violations without user education and training.

QUESTION 346
Which of the following is the MOST effective at preventing an unauthorized individual from following an authorized person through a secured entrance (tailgating or piggybacking)?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. The other choices are physical controls which by themselves would not be effective against tailgating.

QUESTION 347
Data owners will determine what access and authorizations users will have by:

A. delegating authority to data custodian.
B. cloning existing user accounts.
C. determining hierarchical preferences.
D. mapping to business needs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Access and authorizations should be based on business needs. Data custodians implement the decisions made by data owners. Access and authorizations are not to be assigned by cloning existing user accounts or determining hierarchical preferences. By cloning, users may obtain more access rights and privileges than is required to do their job. Hierarchical preferences may be based on individual preferences and not on business needs.

Real 241
Isaca CISM Exam

QUESTION 348
Which of the following is the MOST likely outcome of a well-designed information security awareness course?

A. Increased reporting of security incidents to the incident response function
B. Decreased reporting of security incidents to the incident response function
C. Decrease in the number of password resets

D. Increase in the number of identified system vulnerabilities

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A well-organized information security awareness course informs all employees of existing security policies, the importance of following safe practices for data security anil the need to report any possible security incidents to the appropriate individuals in the organization. The other choices would not be the likely outcomes.

QUESTION 349
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 350
A critical component of a continuous improvement program for information security is:

Real 242
Isaca CISM Exam

A. measuring processes and providing feedback.
B. developing a service level agreement (SLA) for security.
C. tying corporate security standards to a recognized international standard.
D. ensuring regulatory compliance.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 351
The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager

A. report risks in other departments.
B. obtain support from other departments.
C. report significant security risks.

D. have knowledge of security standards.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IT manager needs to report the security risks in the environment pursuant to the security review, including risks in the IT implementation. Choices A, B and D are important, but not the main responsibilities or job requirements.

QUESTION 352
An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

A. Rule-based
B. Mandatory
Real 243
Isaca CISM Exam
C. Discretionary
D. Role-based

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 353
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

A. an audit of the service provider uncovers no significant weakness.
B. the contract includes a nondisclosure agreement (NDA) to protect the organization's intellectual property.
C. the contract should mandate that the service provider will comply with security policies.
D. the third-party service provider conducts regular penetration testing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It is critical to include the security requirements in the contract based ON the company's security policy to ensure that the necessary security controls are implemented by the service provider. The audit is normally a one-time effort and cannot provide ongoing assurance of the security. A nondisclosure agreement (NDA) should be part of the contract; however, it is not critical to the security of the web site. Penetration testing alone would not provide total security to the web site; there are lots of controls that cannot be tested through penetration testing.

QUESTION 354

Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

Real 244
Isaca CISM Exam

A. To mitigate technical risks
B. To have an independent certification of network security
C. To receive an independent view of security exposures
D. To identify a complete list of vulnerabilities

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Even though the organization may have the capability to perform penetration testing with internal resources, third-party penetration testing should be performed to gain an independent view of the security exposure. Mitigating technical risks is not a direct result of a penetration test. A penetration test would not provide certification of network security nor provide a complete list of vulnerabilities.

QUESTION 355
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

A. Prepare an impact assessment report.
B. Conduct a penetration test.
C. Obtain approval from senior management.
D. Back up the firewall configuration and policy files.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 356
An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

A. Request that the third-party provider perform background checks on their employees.
B. Perform an internal risk assessment to determine needed controls.
C. Audit the third-party provider to evaluate their security controls.
   Real 245
   Isaca CISM Exam
D. Perform a security assessment to detect security vulnerabilities.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An internal risk assessment should be performed to identify the risk and determine needed controls. A background check should be a standard requirement for the service provider. Audit objectives should be

determined from the risk assessment results. Security assessment does not cover the operational risks.

QUESTION 357
Which of the following would raise security awareness among an organization's employees?

A. Distributing industry statistics about security incidents
B. Monitoring the magnitude of incidents
C. Encouraging employees to behave in a more conscious manner
D. Continually reinforcing the security policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Employees must be continually made aware of the policy and expectations of their behavior. Choice A would have little relevant bearing on the employee's behavior. Choice B does not involve the employees. Choice C could be an aspect of continual reinforcement of the security policy.

QUESTION 358
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

A. Attempt to reset several passwords to weaker values
B. Install code to capture passwords for periodic audit
C. Sample a subset of users and request their passwords for review
D. Review general security settings on each platform

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reviewing general security settings on each platform will be the most efficient method for

determining password strength while not compromising the integrity of the passwords. Attempting to reset several passwords to weaker values may not highlight certain weaknesses. Installing code to capture passwords for periodic audit, and sampling a subset of users and requesting their passwords for review, would compromise the integrity of the passwords.

QUESTION 359
What is the MOST cost-effective method of identifying new vendor vulnerabilities?

A. External vulnerability reporting sources
B. Periodic vulnerability assessments performed by consultants
C. Intrusion prevention software
D. honey pots located in the DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
External vulnerability sources are going to be the most cost-effective method of identifying these vulnerabilities. The cost involved in choices B and C would be much higher, especially if performed at

regular intervals. Honeypots would not identify all vendor vulnerabilities. In addition, honeypots located in the DMZ can create a security risk if the production network is not well protected from traffic from compromised honey pots.

QUESTION 360
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audits.
B. Perform periodic penetration testing.
C. Define and monitor security metrics.
D. Survey business units for feedback.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Defining and monitoring security metrics is a good approach to analyze the performance of the security management process since it determines the baseline and evaluates the performance against the baseline to identify an opportunity for improvement. This is a systematic and structured

approach to process improvement. Audits will identify deficiencies in established controls; however, they are not effective in evaluating the overall performance for improvement. Penetration testing will only uncover technical vulnerabilities, and cannot provide a holistic picture of information security management, feedback is subjective and not necessarily reflective of true performance.

QUESTION 361
An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

A. validate and sanitize client side inputs.
B. harden the database listener component.
C. normalize the database schema to the third normal form.
D. ensure that the security patches are updated on operating systems.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 362
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
XSRF exploits inadequate authentication mechanisms in web applications that rely only on

Real 248
Isaca CISM Exam

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

QUESTION 363
Of the following, retention of business records should be PRIMARILY based on:

A. periodic vulnerability assessment.
B. regulatory and legal requirements.
C. device storage capacity and longevity.
D. past litigation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 364
An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

A. A due diligence security review of the business partner's security controls
B. Ensuring that the business partner has an effective business continuity program
C. Ensuring that the third party is contractually obligated to all relevant security requirements
D. Talking to other clients of the business partner to check references for performance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The key requirement is that the information security manager ensures that the third party is contractually bound to follow the appropriate security requirements for the process being

Real 249
Isaca CISM Exam

outsourced. This protects both organizations. All other steps are contributory to the contractual agreement, but are not key.

QUESTION 365
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 366
Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regular security audits and reviews of the practices of the provider to prevent potential information security damage will help verify the security of outsourced services. Depending on the type of services outsourced, security awareness may not be necessary. Security requirements should be

included in the contract, but what is most important is verifying that the requirements are met by the provider. It is not necessary to require the provider to fully comply with the policy if only some of the policy is related and applicable.

QUESTION 367
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 368
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
   Real 251
   Isaca CISM Exam
C. A change control process
D. Business impact analysis (BIA)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 369
Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 370
In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

A. Procedural design
Real 252
Isaca CISM Exam
B. Architectural design
C. System design specifications
D. Software development

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The system design specifications phase is when security specifications are identified. The procedural design converts structural components into a procedural description of the software. The architectural design is the phase that identifies the overall system design, hut not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.

QUESTION 371
Which of the following is generally considered a fundamental component of an information security program?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 372
How would an organization know if its new information security program is accomplishing its goals?

A. Key metrics indicate a reduction in incident impacts.
B. Senior management has approved the program and is supportive of it.
C. Employees are receptive to changes that were implemented.
D. There is an immediate reduction in reported incidents.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Real 253
Isaca CISM Exam

Explanation:
Option A is correct since an effective security program will show a trend in impact reduction. Options B and C may well derive from a performing program, but are not as significant as option A. Option D may indicate that it is not successful.

QUESTION 373
A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

A. it simulates the real-1ife situation of an external security attack.
B. human intervention is not required for this type of test.
C. less time is spent on reconnaissance and information gathering.
D. critical infrastructure information is not revealed to the tester.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 374
Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A. Acceptable use policy
B. Setting low mailbox limits
C. User awareness training
D. Taking disciplinary action

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
User awareness training would help in reducing the incidents of employees forwarding spam and chain e-mails since users would understand the risks of doing so and the impact on the

organization's information system. An acceptable use policy, signed by employees, would legally address the requirements but merely having a policy is not the best measure. Setting low mailbox limits and taking disciplinary action are a reactive approach and may not help in obtaining proper support from employees.

QUESTION 375
Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

A. Passwords stored in encrypted form
B. User awareness
C. Strong passwords that are changed periodically
D. Implementation of lock-out policies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Implementation of account lock-out policies significantly inhibits brute-force attacks. In cases where this is not possible, strong passwords that are changed periodically would be an appropriate choice. Passwords stored in encrypted form w ill not defeat an online brute-force attack if the password itself is easily guessed. User awareness would help but is not the best approach of the options given.

QUESTION 376
Which of the following measures is the MOST effective deterrent against disgruntled stall abusing their privileges?

A. Layered defense strategy
B. System audit log monitoring
C. Signed acceptable use policy
D. High-availability systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A layered defense strategy would only prevent those activities that are outside of the user's privileges. A signed acceptable use policy is often an effective deterrent against malicious

activities because of the potential for termination of employment and/or legal actions being taken against the individual. System audit log monitoring is after the fact and may not be effective. High- availability systems have high costs and are not always feasible for all devices and components or systems.

QUESTION 377
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

A. the existence of messages is unknown.
B. required key sizes are smaller.
C. traffic cannot be sniffed.
D. reliability of the data is higher in transit.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The existence of messages is hidden when using steganography. This is the greatest risk. Keys are relevant for encryption and not for steganography. Sniffing of steganographic traffic is also possible. Option D is not relevant.

QUESTION 378
As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A. considered at the discretion of the information owner.
B. approved by the next higher person in the organizational structure.
C. formally managed within the information security framework.
D. reviewed and approved by the security manager.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A formal process for managing exceptions to information security policies and standards should be

included as part of the information security framework. The other options may be contributors to the process but do not in themselves constitute a formal process.

Real 256
Isaca CISM Exam

QUESTION 379
There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

A. Black box pen test
B. Security audit
C. Source code review
D. Vulnerability scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Source code review is the best way to find and remove an application backdoor. Application backdoors can be almost impossible to identify' using a black box pen test or a security audit. A vulnerability scan will only find "known" vulnerability patterns and will therefore not find a programmer's application backdoor.

QUESTION 380
Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does il always introduce?

A. Remote buffer overflow
B. Cross site scripting
C. Clear text authentication
D. Man-in-the-middle attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One of the main problems with using SNMP vl and v°2 is the clear text "community string" that it uses to authenticate. It is easy to sniff and reuse. Most times, the SNMP community string is shared throughout the organization's servers and routers, making this authentication problem a serious threat to security. There have been some isolated cases of remote buffer overflows against SNMP daemons, but generally that is not a problem. Cross site scripting is a web application vulnerability that is not related to SNMP. A man-in-the-middlc attack against a user datagram protocol (UDP) makes no sense since there is no active session; every request has the

Real 257
Isaca CISM Exam

community string and is answered independently.

QUESTION 381
Which of the following is the FIRST phase in which security should be addressed in the development cycle of a project?

A. Design
B. Implementation
C. Application security testing
D. Feasibility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security should be considered at the earliest possible stage. Security requirements must be defined before you enter into design specification, although changes in design may alter these requirements later on. Security requirements defined during system implementation are typically costly add-ons that are frequently ineffective. Application security testing occurs after security has been implemented.

Topic 5, INCIDENT MANAGEMENT AND RESPONSE

QUESTION 382
Which of the following should be determined FIRST when establishing a business continuity program?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Prior to creating a detailed business continuity plan, it is important to determine the incremental

daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION 383
A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. disconnecting the computer from all power sources.
B. disabling all local user accounts except for one administrator.
C. encrypting local files and uploading exact copies to a secure server.
D. copying all files using the operating system (OS) to write-once media.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing it remotely changes the operating system (OS) and temporary files on the computer and invalidates it as admissible evidence.

QUESTION 384
A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GRF.ATEST weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks
B. The hot site may have to be shared with other customers
C. The time of declaration determines site access priority
D. The provider services all major companies in the area

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. Access to a

Real 259
Isaca CISM Exam

hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

QUESTION 385
Which of the following actions should be taken when an online trading company discovers a network attack in progress?

A. Shut off all network access points
B. Dump all event logs to removable media
C. Isolate the affected network segment
D. Enable trace logging on all event

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

QUESTION 386
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.
B. bastion hosts.
C. decoy files.
D. screened subnets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Decoy files, often referred to as honcypots, are the best choice for diverting a hacker away from

Real 260

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

QUESTION 387
The FIRST priority when responding to a major security incident is:

A. documentation.
B. monitoring.
C. restoration.
D. containment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The first priority in responding to a security incident is to contain it to limit the impact. Documentation, monitoring and restoration are all important, but they should follow containment.

QUESTION 388
Which of the following is the MOST important to ensure a successful recovery?

A. Backup media is stored offsite
B. Recovery location is secure and accessible
C. More than one hot site is available
D. Network alternate links are regularly tested

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Unless backup media are available, all other preparations become meaningless. Recovery site location and security are important, but would not prevent recovery in a disaster situation. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, alternate data communication lines should be tested regularly and successfully but, again, this is not as critical.

Real 261
Isaca CISM Exam

QUESTION 389
Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot site?

A. Tests are scheduled on weekends
B. Network IP addresses are predefined
C. Equipment at the hot site is identical
D. Business management actively participates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Disaster recovery testing requires the allocation of sufficient resources to be successful. Without the

support of management, these resources will not be available, and testing will suffer as a result. Testing on weekends can be advantageous but this is not the most important choice. As vendor-provided hot sites are in a state of constant change, it is not always possible to have network addresses defined in advance. Although it would be ideal to provide for identical equipment at the hot site, this is not always practical as multiple customers must be served and equipment specifications will therefore vary.

QUESTION 390
At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

A. Erase data and software from devices
B. Conduct a meeting to evaluate the test
C. Complete an assessment of the hot site provider
D. Evaluate the results from all test scripts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations can occur back at the office after everyone is rested, and the overall results can be discussed and compared objectively.

QUESTION 391
Real 262
Isaca CISM Exam
An incident response policy must contain:

A. updated call trees.
B. escalation criteria.
C. press release templates.
D. critical backup files inventory.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 392
The BEST approach in managing a security incident involving a successful penetration should be to:

A. allow business processes to continue during the response.
B. allow the security team to assess the attack profile.
C. permit the incident to continue to trace the source.
D. examine the incident response process for deficiencies.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since information security objectives should always be linked to the objectives of the business, it is

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

QUESTION 393
A post-incident review should be conducted by an incident management team to determine:

Real 263
Isaca CISM Exam

A. relevant electronic evidence.
B. lessons learned.
C. hacker's identity.
D. areas affected.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Post-incident reviews are beneficial in determining ways to improve the response process through lessons learned from the attack. Evaluating the relevance of evidence, who launched the attack or what areas were affected are not the primary purposes for such a meeting because these should have been already established during the response to the incident.

QUESTION 394
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 centers.
B. current processing capacity loads at data centers.
C. differences in logical security at each center.
D. synchronization of system software release versions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 395
Which of the following is MOST important in determining whether a disaster recovery test is successful?

A. Only business data files from offsite storage are used
B. IT staff fully recovers the processing infrastructure
C. Critical business processes are duplicated
   Real 264
   Isaca CISM Exam
D. All systems are restored within recovery time objectives (RTOs)

Correct Answer: C

Section: (none)
Explanation

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

QUESTION 396
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 397
Real 265
Isaca CISM Exam
A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 398
When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall
B. Power down all servers located on the DMZ segment
C. Monitor the probe and isolate the affected segment
D. Enable server trace logging on the affected segment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the demilitarized zone (DMZ) servers and enabling server trace routing are not warranted.

QUESTION 399
Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

Real 266
Isaca CISM Exam

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 400
Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 401

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

A. Detailed technical recovery plans are maintained offsite Real 267
Isaca CISM Exam
B. Network redundancy is maintained through separate providers
C. Hot site equipment needs are recertified on a regular basis
D. Appropriate declaration criteria have been established

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 402
The business continuity policy should contain which of the following?

A. Emergency call trees
B. Recovery criteria
C. Business impact assessment (BIA)
D. Critical backups inventory

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

QUESTION 403
The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

A. weaknesses in network security.
B. patterns of suspicious access.
C. how an attack was launched on the network.
Real 268
Isaca CISM Exam
D. potential attacks on the internal network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 404
When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

A. Ensuring accessibility should a disaster occur
B. Versioning control as plans are modified
C. Broken hyperlinks to resources stored elsewhere
D. Tracking changes in personnel and plan assets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

QUESTION 405
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 269
Isaca CISM Exam

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.

QUESTION 406
Which of the following actions should be taken when an information security manager discovers that a hacker is foot printing the network perimeter?

A. Reboot the border router connected to the firewall
B. Check IDS logs and monitor for any active attacks
C. Update IDS software to the latest available version
D. Enable server trace logging on the DMZ segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security should check the intrusion detection system (IDS) logs and continue to monitor the situation. It would be inappropriate to take any action beyond that. In fact, updating the IDS could create a

temporary exposure until the new version can be properly tuned. Rebooting the router and enabling server trace routing would not be warranted.

QUESTION 407
Which of the following are the MOST important criteria when selecting virus protection software?

A. Product market share and annualized cost
B. Ability to interface with intrusion detection system (IDS) software and firewalls
C. Alert notifications and impact assessments for new viruses
D. Ease of maintenance and frequency of updates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For the software to be effective, it must be easy to maintain and keep current. Market share and annualized cost, links to the intrusion detection system (IDS) and automatic notifications are all secondary in nature.

Real 270
Isaca CISM Exam

QUESTION 408
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 409
When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

A. Business continuity coordinator
B. Information security manager
C. Business process owners
D. Industry averages benchmarks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business process owners are in the best position to understand the true impact on the business that a system outage would create. The business continuity coordinator, industry averages and even information security will not be able to provide that level of detailed knowledge.

QUESTION 410
Real 271
Isaca CISM Exam
Which of the following is MOST closely associated with a business continuity program?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 411
Which of the following application systems should have the shortest recovery time objective (RTO)?

A. Contractor payroll
B. Change management
C. E-commerce web site
D. Fixed asset system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours, if not minutes. Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

QUESTION 412
A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

A. Risk assessment results
B. Severity criteria
C. Emergency call tree directory
Real 272
Isaca CISM Exam
D. Table of critical backup files

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 413
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 security.
B. ways to improve the incident response process.
C. potential attack vectors on the network perimeter.
D. the optimum response to internal hacker attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 414
Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

A. removed into the custody of law enforcement investigators.
B. kept in the tape library' pending further analysis.
C. sealed in a signed envelope and locked in a safe under dual control.
D. handed over to authorized independent investigators.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since a number of individuals would have access to the tape library, and could have accessed and tampered with the tape, the chain of custody could not be verified. All other choices provide clear indication of who was in custody of the tape at all times.

Real 273
Isaca CISM Exam

QUESTION 415
When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 416
Isolation and containment measures lor a compromised computer have been taken and information security management is now investigating. What is the MOST appropriate next step?

A. Run a forensics tool on the machine to gather evidence
B. Reboot the machine to break remote connections
C. Make a copy of the whole system's memory
D. Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/I'DP) ports

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When investigating a security breach, it is important to preserve all traces of evidence left by the invader. For this reason, it is imperative to preserve the memory' contents of the machine in order to analyze them later. The correct answer is choice C because a copy of the whole system's memory is obtained for future analysis by running the appropriate tools. This is also important from

a legal perspective since an attorney may suggest that the system was changed during the conduct of the investigation. Running a computer forensics tool in the compromised machine will cause the creation of at least one process that may overwrite evidence. Rebooting the machine will delete the contents of the memory, erasing potential evidence. Collecting information about current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports is correct, but doing so by using tools may also erase memory contents.

QUESTION 417
Why is "slack space" of value to an information security manager as pan of an incident investigation?

A. Hidden data may be stored there
B. The slack space contains login information
C. Slack space is encrypted
D. It provides flexible space for the investigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"Slack space" is the unused space between where the fdc data end and the end of the cluster the data occupy. Login information is not typically stored in the slack space. Encryption for the slack space is no different from the rest of the file system. The slack space is not a viable means of storage during an investigation.

QUESTION 418
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Real 275
Isaca CISM Exam

QUESTION 419
Detailed business continuity plans should be based PRIMARILY on:

A. consideration of different alternatives.
B. the solution that is least expensive.
C. strategies that cover all applications.
D. strategies validated by senior management.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 420
A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. rebuild the server from the last verified backup.
B. place the web server in quarantine.
C. shut down the server in an organized manner.
D. rebuild the server with original media and relevant patches.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last

Real 276
Isaca CISM Exam

known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

QUESTION 421
Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

A. A bit-level copy of all hard drive data

B. The last verified backup stored offsite
C. Data from volatile memory
D. Backup servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The bit-level copy image file ensures forensic quality evidence that is admissible in a court of law. Choices B and D may not provide forensic quality data for investigative work, while choice C alone may not provide enough evidence.

QUESTION 422
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 standards.
B. local regulations.
C. generally accepted best practices.
D. organizational security policies.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 423
Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

A. determining the extent of property damage.
B. preserving environmental conditions.
C. ensuring orderly plan activation.
D. reducing the extent of operational damage.

Correct Answer: D
Section: (none)
Explanation

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

not as critical as reducing damage to the operation.

QUESTION 424
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

Correct Answer: C
Section: (none)
Explanation

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

Real 278
Isaca CISM Exam

QUESTION 425
Which of the following actions should lake place immediately after a security breach is reported to an information security manager?

A. Confirm the incident
B. Determine impact
C. Notify affected stakeholders
D. Isolate the incident

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Before performing analysis of impact, resolution, notification or isolation of an incident, ii must be validated as a real security incident.

QUESTION 426
When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

A. services delivery objective.
B. recovery time objective (RTO).
C. recovery window.
D. maximum tolerable outage (MTO).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The length of the recovery window is defined by business management and determines the acceptable time frame between a disaster and the restoration of critical services/applications. The technical implementation of the disaster recovery (DR) site will be based on this constraint, especially the choice between a hot, warm or cold site. The service delivery objective is supported during the alternate process mode until the normal situation is restored, which is directly related to business needs. The recovery time

objective (RTO) is commonly agreed to be the time frame between a disaster and the return to normal operations. It is then longer than the interruption window and is very difficult to estimate in advance. The time frame between the reduced operation mode at the end of the interruption window and the return to normal operations depends on the

Real 279
Isaca CISM Exam

magnitude of the disaster. Technical disaster recovery solutions alone will not be used for returning to normal operations. Maximum tolerable outage (MTO) is the maximum time acceptable by a company operating in reduced mode before experiencing losses. Theoretically, recovery time objectives (RTOs) equal the interruption window plus the maximum tolerable outage. This will not be the primary factor for the choice of the technical disaster recovery solution.

QUESTION 427
In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 428
An intrusion detection system (IDS) should:

A. run continuously
B. ignore anomalies
C. require a stable, rarely changed environment
D. be located on the network
Real 280
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If an intrusion detection system (IDS) does not run continuously the business remains vulnerable. An IDS should detect, not ignore anomalies. An IDS should be flexible enough to cope with a changing environment. Both host and network based IDS are recommended for adequate detection.

QUESTION 429
The PRIORITY action to be taken when a server is infected with a virus is to:

A. isolate the infected server(s) from the network.

B. identify all potential damage caused by the infection.
C. ensure that the virus database files are current.
D. establish security weaknesses in the firewall.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 430
Which of the following provides the BKST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

A. The recovery time objective (RTO) was not exceeded during testing
B. Objective testing of the business continuity/disaster recovery plan has been carried out consistently
C. The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
D. Information assets have been valued and assigned to owners per the business continuity plan, disaster recovery plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 281
Isaca CISM Exam

Consistent achievement of recovery time objective (RTO) objectives during testing provides the most objective evidence that business continuity/disaster recovery plan objectives have been achieved. The successful testing of the business continuity/disaster recover) plan within the stated RTO objectives is the most indicative evidence that the business needs are being met. Objective testing of the business continuity/ disaster recovery plan will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning.. Mere valuation and assignment of information assets to owners (per the business continuity/disaster recovery plan) will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning.

QUESTION 431
Which of the following situations would be the MOST concern to a security manager?

A. Audit logs are not enabled on a production server
B. The logon ID for a terminated systems analyst still exists on the system
C. The help desk has received numerous results of users receiving phishing e-mails
D. A Trojan was found to be installed on a system administrator's laptop

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The discovery of a Trojan installed on a system's administrator's laptop is highly significant since this may mean that privileged user accounts and passwords may have been compromised. The other choices, although important, do not pose as immediate or as critical a threat.

QUESTION 432
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. confirm the incident.
B. notify senior management.
C. start containment.
D. notify law enforcement.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 282
Isaca CISM Exam

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.

QUESTION 433
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 occurred.
B. notify law enforcement.
C. take an image copy of the media.
D. close the accounts receivable system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 434
When collecting evidence for forensic analysis, it is important to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Real 283
Isaca CISM Exam

QUESTION 435
What is the BEST method for mitigating against network denial of service (DoS) attacks?

A. Ensure all servers are up-to-date on OS patches
B. Employ packet filtering to drop suspect packets
C. Implement network address translation to make internal addresses nonroutable
D. Implement load balancing for Internet facing devices

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Packet filtering techniques are the only ones which reduce network congestion caused by a network denial of service (DoS) attack. Patching servers, in general, will not affect network traffic. Implementing network address translation and load balancing would not be as effective in mitigating most network DoS attacks.

QUESTION 436
To justify the establishment of an incident management team, an information security manager would find which of the following to be the MOST effective?

A. Assessment of business impact of past incidents
B. Need of an independent review of incident causes
C. Need for constant improvement on the security level
D. Possible business benefits from incident impact reduction

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business benefits from incident impact reduction would be the most important goal for establishing an incident management team. The assessment of business impact of past incidents would need to be completed to articulate the benefits. Having an independent review benefits the incident management process. The need for constant improvement on the security level is a benefit to the organization.

Real 284
Isaca CISM Exam

QUESTION 437
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts
B. Write access violations
C. Concurrent logons
D. Firewall logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since the password for the shared administrative account was obtained through guessing, it is probable

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

QUESTION 438
Which of the following is an example of a corrective control?

A. Diverting incoming traffic upon responding to the denial of service (DoS) attack
B. Filtering network traffic before entering an internal network from outside
C. Examining inbound network traffic for viruses
D. Logging inbound network traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Diverting incoming traffic corrects the situation and. therefore, is a corrective control. Choice B is a preventive control. Choices C and D are detective controls.

QUESTION 439
To determine how a security breach occurred on the corporate network, a security manager looks

at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

A. Database server
B. Domain name server (DNS)
C. Time server
D. Proxy server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To accurately reconstruct the course of events, a time reference is needed and that is provided by the time server. The other choices would not assist in the correlation and review1 of these logs.

QUESTION 440
An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 441
A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

Real 286
Isaca CISM Exam

A. Ensure that all OS patches are up-to-date
B. Block inbound traffic until a suitable solution is found
C. Obtain guidance from the firewall manufacturer
D. Commission a penetration test

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring dial all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

QUESTION 442
An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

A. use the test equipment in the warm site facility to read the tapes.
B. retrieve the tapes from the warm site and test them.
C. have duplicate equipment available at the warm site.
D. inspect the facility and inventory the tapes on a quarterly basis.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A warm site is not fully equipped with the company's main systems; therefore, the tapes should be tested using the company's production systems. Inspecting the facility and checking the tape inventory does not guarantee that the tapes are usable.

QUESTION 443
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

A. Business impact analysis (BIA)
B. Risk assessment
   Real 287
   Isaca CISM Exam
C. Vulnerability assessment

D. Business process mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A business impact analysis (BIA) provides results, such as impact from a security incident and required response times. The BIA is the most critical process for deciding which part of the information system/ business process should be given prioritization in case of a security incident. Risk assessment is a very important process for the creation of a business continuity plan. Risk assessment provides information on the likelihood of occurrence of security incidence and assists in the selection of countermeasures. but not in the prioritization. As in choice B, a vulnerability assessment provides information regarding the security weaknesses of the system, supporting the risk analysis process. Business process mapping facilitates the creation of the plan by providing mapping guidance on actions after the decision on critical business processes has been made- translating business prioritization to IT prioritization. Business process mapping does not help in making a decision, but in implementing a decision.

QUESTION 444
In addition to backup data, which of the following is the MOST important to store offsite in the event of a disaster?

A. Copies of critical contracts and service level agreements (SLAs)
B. Copies of the business continuity plan
C. Key software escrow agreements for the purchased systems
D. List of emergency numbers of service providers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Without a copy of the business continuity plan, recovery efforts would be severely hampered or may not be effective. All other choices would not be as immediately critical as the business continuity plan itself. The business continuity plan would contain a list of the emergency numbers of service providers.

QUESTION 445
An organization has learned of a security breach at another company that utilizes similar

technology. The FIRST thing the information security manager should do is:

A. assess the likelihood of incidents from the reported cause.
B. discontinue the use of the vulnerable technology.
C. report to senior management that the organization is not affected.
D. remind staff that no similar security breaches have taken place.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 446
Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 447
During the security review of organizational servers it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the

Real 289
Isaca CISM Exam
security manager should:

A. copy sample files as evidence.
B. remove access privileges to the folder containing the data.
C. report this situation to the data owner.
D. train the HR team on properly controlling file permissions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The data owner should be notified prior to any action being taken. Copying sample files as evidence is not advisable since it breaches confidentiality requirements on the file. Removing access privileges to the folder containing the data should be done by the data owner or by the security manager in consultation with the data owner, however, this would be done only after formally reporting the incident. Training the human resources (MR) team on properly controlling file permissions is the method to prevent such incidents in the future, but should take place once the incident reporting and investigation activities are completed.

QUESTION 448
If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A. obtaining evidence as soon as possible.
B. preserving the integrity of the evidence.
C. disconnecting all IT equipment involved.
D. reconstructing the sequence of events.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are pan of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

QUESTION 449
Which of the following has the highest priority when defining an emergency response plan?

Real 290
Isaca CISM Exam

A. Critical data
B. Critical infrastructure
C. Safety of personnel
D. Vital records

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

QUESTION 450
The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 451
The MOST important objective of a post incident review is to:

A. capture lessons learned to improve the process.
B. develop a process for continuous improvement.
C. develop a business case for the security program budget.
D. identify new incident management tools.
Real 291
Isaca CISM Exam

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 452
Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 453
The FIRST step in an incident response plan is to:

A. notify- the appropriate individuals.
B. contain the effects of the incident to limit damage.
C. develop response strategies for systematic attacks.
D. validate the incident.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Appropriate people need to be notified; however, one must first validate the incident. Containing the effects of the incident would be completed after validating the incident. Developing response strategies for systematic attacks should have already been developed prior to the occurrence of

Real 292
Isaca CISM Exam

an incident.

QUESTION 454
An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

A. Inform senior management.
B. Determine the extent of the compromise.
C. Report the incident to the authorities.
D. Communicate with the affected customers.

Correct Answer: B
Section: (none)

Explanation

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

QUESTION 455
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 456
Real 293
Isaca CISM Exam
The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

A. regulatory' requirements.
B. business requirements.
C. financial value.
D. IT resource availability.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The criticality to business should always drive the decision. Regulatory requirements could be more flexible than business needs. The financial value of an asset could not correspond to its business value. While a consideration, IT resource availability is not a primary factor.

QUESTION 457
What task should be performed once a security incident has been verified?

A. Identify the incident.
B. Contain the incident.
C. Determine the root cause of the incident.
D. Perform a vulnerability assessment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 458
An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

A. Unsure that critical data on the server are backed up.
   Real 294
   Isaca CISM Exam
B. Shut down the compromised server.
C. Initiate the incident response process.
D. Shut down the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

QUESTION 459
An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

A. Shut down and power off the server.
B. Duplicate the hard disk of the server immediately.
C. Isolate the server from the network.
D. Copy the database log file to a protected server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Isolating the server will prevent further intrusions and protect evidence of intrusion activities left in memory and on the hard drive. Some intrusion activities left in virtual memory may be lost if the system is shut down. Duplicating the hard disk will only preserve the evidence on the hard disk, not the evidence in virtual memory, and will not prevent further unauthorized access attempts. Copying the database log file to a protected server will not provide sufficient evidence should the organization choose to pursue legal recourse.

QUESTION 460
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
   Real 295
   Isaca CISM Exam
B. Maintaining redundant systems
C. Aligning with recovery time objectives (RTOs)
D. Data backup frequency

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 461
Which of the following would be MOST appropriate for collecting and preserving evidence?

A. Encrypted hard drives
B. Generic audit software
C. Proven forensic processes
D. Log correlation software

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When collecting evidence about a security incident, it is very important to follow appropriate forensic procedures to handle electronic evidence by a method approved by local jurisdictions. All other options will help when collecting or preserving data about the incident; however these data might not be accepted as evidence in a court of law if they are not collected by a method approved by local jurisdictions.

QUESTION 462
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Real 296
Isaca CISM Exam

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.

QUESTION 463
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 media.
B. Perform a bit-by-bit image of the original media source onto new media.
C. Make a copy of all files that are relevant to the investigation.

D. Run an error-checking program on all logical drives to ensure that there are no disk errors.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 464
Which of the following recovery strategies has the GREATEST chance of failure?

A. Hot site
B. Redundant site
   Real 297
   Isaca CISM Exam
C. Reciprocal arrangement
D. Cold site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A reciprocal arrangement is an agreement that allows two organizations to back up each other during a disaster. This approach sounds desirable, but has the greatest chance of failure due to problems in keeping agreements and plans up to date. A hot site is incorrect because it is a site kept fully equipped with processing capabilities and other services by the vendor. A redundant site is incorrect because it is a site equipped and configured exactly like the primary site. A cold site is incorrect because it is a building having a basic environment such as electrical wiring, air conditioning, flooring, etc. and is ready to receive equipment in order to operate.

QUESTION 465
Recovery point objectives (RPOs) can be used to determine which of the following?

A. Maximum tolerable period of data loss
B. Maximum tolerable downtime
C. Baseline for operational resiliency
D. Time to restore backups

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The RPO is determined based on the acceptable data loss in the case of disruption of operations. It indicates the farthest point in time prior to the incident to which it is acceptable to recover the data. RPO effectively quantifies the permissible amount of data loss in the case of interruption. It also dictates the frequency of backups required for a given data set since the smaller the allowable gap in data, the more frequent that backups must occur.

QUESTION 466
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
Real 298
Isaca CISM Exam
C. Full operational tests
D. Actual service disruption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 467
When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 468
When creating a forensic image of a hard drive, which of the following should be the FIRST step?

A. Identify a recognized forensics software tool to create the image.
Real 299
Isaca CISM Exam
B. Establish a chain of custody log.
C. Connect the hard drive to a write blocker.
D. Generate a cryptographic hash of the hard drive contents.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Real 300