CISM

Number: CISM
Passing Score: 800
Time Limit: 120 min
File Version: 1

CISM

Sections

1. INFORMATION SECURITY GOVERNANCE
2. INFORMATION RISK MANAGEMENT
3. INFORMATION SECURITY PROGRAM DEVELOPMENT
4. INFORMATION SECURITY PROGRAM MANAGEMENT
5. INCIDENT MANAGEMENT AND RESPONSE

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: INFORMATION SECURITY GOVERNANCE
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
Information security governance is PRIMARILY driven by:

A. technology constraints.
B. regulatory requirements.
C. litigation potential.
D. business strategy.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily in line with the business strategy.

QUESTION 3
Which of the following represents the MAJOR focus of privacy regulations?

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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

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

A. vulnerability assessments.
B. value analysis.
C. business climate.
D. audit recommendations.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
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
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: INFORMATION SECURITY GOVERNANCE
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 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 6
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: INFORMATION SECURITY GOVERNANCE
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 7
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: INFORMATION SECURITY GOVERNANCE
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 8
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: INFORMATION SECURITY GOVERNANCE
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.

QUESTION 9
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: INFORMATION SECURITY GOVERNANCE
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 10
When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 11
It is MOST important that information security architecture be aligned with which of the following?

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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 12
Which of the following is MOST likely to be discretionary?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
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 13
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: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
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 14
Which of the following are seldom changed in response to technological changes?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
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 15
The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

A. storage capacity and shelf life.

B. regulatory and legal requirements.
C. business strategy and direction.
D. application systems and media.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Long-term retention of business records may be severely impacted by changes in application systems and media. For example, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply, nor do legal and regulatory requirements. Storage capacity and shelf life are important but secondary issues.

QUESTION 16
Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 17
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: INFORMATION SECURITY GOVERNANCE
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 18
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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
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 19
Which of the following are likely to be updated MOST frequently?

A. Procedures for hardening database servers
B. Standards for password length and complexity
C. Policies addressing information security governance
D. Standards for document retention and destruction
Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 20
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: INFORMATION SECURITY GOVERNANCE
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 21
When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

A. aligned with the IT strategic plan.
B. based on the current rate of technological change.
C. three-to-five years for both hardware and software.
D. aligned with the business strategy.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:
Explanation:

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

QUESTION 22
Information security projects should be prioritized on the basis of:

A. time required for implementation.
B. impact on the organization.
C. total cost for implementation.
D. mix of resources required.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
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 23
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: INFORMATION SECURITY GOVERNANCE
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 24
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks
C. Demonstrate that IT mitigating controls are in place D. Suggest new IT controls to mitigate operational risk

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The job of the information security officer on such a team is to assess the risks to the business operation. Choice A is incorrect because information security is not limited to IT issues. Choice C is incorrect because at the time a team is formed to assess risk, it is premature to assume that any demonstration of IT controls will mitigate business operations risk. Choice D is incorrect because it is premature at the time of the formation of the team to assume that any suggestion of new IT controls will mitigate business operational risk.

QUESTION 25

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: INFORMATION SECURITY GOVERNANCE
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 26
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 27

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: INFORMATION SECURITY GOVERNANCE
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.

QUESTION 28
While implementing information security governance an organization should FIRST:

A. adopt security standards.
B. determine security baselines.
C. define the security strategy.
D. establish security policies.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The first step in implementing information security governance is to define the security strategy based on which security baselines are determined. Adopting suitable security- standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

QUESTION 29
The MOST basic requirement for an information security governance program is to:

A. be aligned with the corporate business strategy.

B. be based on a sound risk management approach.
C. provide adequate regulatory compliance.
D. provide best practices for security- initiatives.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 30
When designing an information security quarterly report to management, the MOST important element to be considered should be the:

A. information security metrics.
B. knowledge required to analyze each issue.
C. linkage to business area objectives.
D. baseline against which metrics are evaluated.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 31
A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

A. meet with stakeholders to decide how to comply.
B. analyze key risks in the compliance process.
C. assess whether existing controls meet the regulation.
D. update the existing security/privacy policy.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 32

B.

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

When requested

At testing

C. At programming

D. At detail requirements

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
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 33
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: INFORMATION SECURITY GOVERNANCE
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.

C.

QUESTION 34
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.
enforce baseline security levels across the organization.
ensure that security processes are fully documented.
D. implement monitoring of key performance indicators for security processes.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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 35
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

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

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C

D.

is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

QUESTION 36
Who is ultimately responsible for the organization's information?

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

E.

Chief information officer (CIO)

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
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 37
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: INFORMATION SECURITY GOVERNANCE
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.

QUESTION 38
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees

B. Distance between physical locations
C. Complexity of organizational structure
D. Organizational budget

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance. Organizational budget is not a major impact once good governance models are in place; hence governance will help in effective management of the organization's budget.

QUESTION 39
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

A. it implies compliance risks.
B. short-term impact cannot be determined.
C. it violates industry security practices.
D. changes in the roles matrix cannot be detected.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 40
An outcome of effective security governance is:

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

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
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 41
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: INFORMATION SECURITY GOVERNANCE
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 42
Which of the following is the MOST important to keep in mind when assessing the value of information?

A. The potential financial loss

B. The cost of recreating the information
C. The cost of insurance coverage
D. Regulatory requirement
Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The potential for financial loss is always a key factor when assessing the value of information. Choices B, C and D may be contributors, but not the key factor.

QUESTION 43
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 44
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: INFORMATION SECURITY GOVERNANCE
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. 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 45
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: INFORMATION SECURITY GOVERNANCE
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 46
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: INFORMATION SECURITY GOVERNANCE
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 47
When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

A. Business management
B. Operations manager
C. Information security manager
D. System users

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

QUESTION 48
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: INFORMATION SECURITY GOVERNANCE
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 49
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: INFORMATION SECURITY GOVERNANCE
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 50
When developing an information security program, what is the MOST useful source of information for determining available resources?

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

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
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 51
An information security manager must understand the relationship between information security and business operations in order to:

A. support organizational objectives.
B. determine likely areas of noncompliance.
C. assess the possible impacts of compromise.
D. understand the threats to the business.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 52
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: INFORMATION SECURITY GOVERNANCE
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 53
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

A. establishing a periodic risk assessment.
B. promoting regulatory requirements.
C. developing a business case.
D. developing effective metrics.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 54
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: INFORMATION SECURITY GOVERNANCE
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 55
Which of the following is the MOST important element of an information security strategy?

A. Defined objectives
B. Time frames for delivery
C. Adoption of a control framework
D. Complete policies

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
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 56
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

A. Representation by regional business leaders
B. Composition of the board
C. Cultures of the different countries
D. IT security skills

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Culture has a significant impact on how information security will be implemented. Representation by regional business leaders may not have a major influence unless it concerns cultural issues. Composition of the board may not have a significant impact compared to cultural issues. IT security skills are not as key or high impact in designing a multinational information security program as would be cultural issues.

QUESTION 57
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: INFORMATION SECURITY GOVERNANCE
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 58
The MOST important factor in ensuring the success of an information security program is effective:

A. communication of information security requirements to all users in the organization.
B. formulation of policies and procedures for information security.
C. alignment with organizational goals and objectives.
D. monitoring compliance with information security policies and procedures.

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The success of security programs is dependent upon alignment with organizational goals and objectives. Communication is a secondary step. Effective communication and education of users is a critical determinant of success but alignment with organizational goals and objectives is the most important factor for success. Mere formulation of policies without effective communication to users will not ensure success. Monitoring compliance with information security policies and procedures can be, at best, a detective mechanism that will not lead to success in the midst of uninformed users.

QUESTION 59
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: INFORMATION SECURITY GOVERNANCE
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-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 60
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: INFORMATION SECURITY GOVERNANCE
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 importance is secondary and will vary depending on organizational goals.

QUESTION 61
Which of the following is the **BEST** advantage of a centralized information security organizational structure?
A. It allows for a common level of assurance across the enterprise.
B. It is easier to manage and control business unit security teams.
C. It is more responsive to business unit needs.
D. It provides a faster turnaround for security waiver requests.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
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 62
The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

A. return on investment (ROD.
B. a vulnerability assessment.
C. annual loss expectancy (ALE).
D. a business case.

Correct Answer: D

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

A business case shows both direct and indirect benefits, along with the investment required and the expected returns, thus making it useful to present to senior management. Return on investment (ROD would only provide the costs needed to preclude specific risks, and would not provide other indirect benefits such as process improvement and learning. A vulnerability assessment is more technical in nature and would only identify and assess the vulnerabilities. This would also not provide insights on indirect benefits. Annual loss expectancy (ALE) would not weigh the advantages of implementing single sign-on (SSO) in comparison to the cost of implementation.

QUESTION 63
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: INFORMATION SECURITY GOVERNANCE
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 64
Which of the following is a benefit of information security governance?

A. Reduction of the potential for civil or legal liability
B. Questioning trust in vendor relationships
C. Increasing the risk of decisions based on incomplete management information
D. Direct involvement of senior management in developing control processes

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Information security governance decreases the risk of civil or legal liability. The remaining answers are incorrect. Option D appears to be correct, but senior management would provide oversight and approval as opposed to direct involvement in developing control processes.

QUESTION 65
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: INFORMATION SECURITY GOVERNANCE
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 66
The data access requirements for an application should be determined by the:

A. legal department.
B. compliance officer.
C. information security manager.
D. business owner.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 67
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: INFORMATION SECURITY GOVERNANCE
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 68
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: INFORMATION SECURITY GOVERNANCE
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 69
Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

A. Obtain the support of the board of directors.
B. Improve the content of the information security awareness program.
C. Improve the employees' knowledge of security policies.

D. Implement logical access controls to the information systems.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 70
A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will own the process regarding the results and the assigned risk. Which of the following would be the BEST approach of the information security manager?

A. Acceptance of the business manager's decision on the risk to the corporation
B. Acceptance of the information security manager's decision on the risk to the corporation
C. Review of the assessment with executive management for final input
D. A new risk assessment and BIA are needed to resolve the disagreement

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

Executive management must be supportive of the process and fully understand and agree with the results since risk management decisions can often have a large financial impact and require major changes. Risk management means different things to different people, depending upon their role in the organization, so the input of executive management is important to the process.

QUESTION 71
What is the MOST important factor in the successful implementation of an enterprise wide information security program?

C.

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

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 72
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: INFORMATION SECURITY GOVERNANCE
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 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 73

C.

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.
departmental budgets are allocated appropriately to pay for the plan.
regulatory oversight requirements are met.
D. the impact of the plan on the business units is reduced.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
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 74
When implementing effective security governance within the requirements of the company's security strategy, which of the following is the MOST important factor to consider?

A. Preserving the confidentiality of sensitive data
B. Establishing international security standards for data sharing
C. Adhering to corporate privacy standards
D. Establishing system manager responsibility for information security

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
Explanation:

The goal of information security is to protect the organization's information assets. International security standards are situational, depending upon the company and its business. Adhering to corporate privacy standards is important, but those standards must be appropriate and adequate and are not the most important factor to consider. All employees are responsible for information security, but it is not the most important factor to consider.

C.

QUESTION 75
Which of the following is the BEST reason to perform a business impact analysis (BIA)?

A. To help determine the current state of risk
To budget appropriately for needed controls

C.

To satisfy regulatory requirements

D. To analyze the effect on the business

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
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 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.

QUESTION 76
Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

A. An emerging technologies strategy is in place
B. An effective security risk management process is established
C. End user acceptance of emerging technologies is established
D. A cost-benefit analysis process is easier to perform

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 77
Which of the following is the MOST appropriate board-level activity for information security governance?

A. Establish security and continuity ownership
B. Develop “what-if” scenarios on incidents
C. Establish measures for security baselines
D. Include security in job-performance appraisals

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 78
Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

A. Implementing additional security awareness training
B. Communicating critical risk assessment results to business unit managers
C. Including business unit representation on the security steering committee
D. Publishing updated information security policies

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 79
In addition to business alignment and security ownership, which of the following is MOST critical for information security governance?

A. Auditability of systems
B. Compliance with policies
C. Reporting of security metrics
D. Executive sponsorship

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 80

Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

A. Areas of highest risk may not be adequately prioritized for treatment
B. Redundant controls may be implemented across divisions
C. Information security governance could be decentralized by division
D. Return on investment may be inconsistently reported to senior management

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 81
The effectiveness of an information security governance framework will BEST be enhanced if:

A. IS auditors are empowered to evaluate governance activities
B. risk management is built into operational and strategic activities
C. a culture of legal and regulatory compliance is promoted by management
D. consultants review the information security governance framework

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 82
When developing an information security governance framework, which of the following would be the **MAIN** impact when lacking senior management involvement?

A. Accountability for risk treatment is not clearly defined.
B. Information security responsibilities are not communicated effectively.
C. Resource requirements are not adequately considered.
D. Information security plans do not support business requirements.

Correct Answer: C

Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:

QUESTION 83
Which of the following is the **BEST** way to facilitate the alignment between an organization's information security program and business objectives?

A. Information security is considered at the feasibility stage of all IT projects.
B. The information security governance committee includes representation from key business areas.
C. The chief executive officer reviews and approves the information security program.
D. The information security program is audited by the internal audit department.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 84
The effectiveness of the information security process is reduced when an outsourcing organization:

A. is responsible for information security governance activities
B. receives additional revenue when security service levels are met
C. incurs penalties for failure to meet security service-level agreements
D. standardizes on a single access-control software product

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 85
What should be an information security manager's **FIRST** course of action when an organization is subject to a new regulatory requirement?

A. Perform a gap analysis

B. Complete a control assessment
C. Submit a business case to support compliance
D. Update the risk register

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 86
Which of the following is the **MOST** important reason for an organization to develop an information security governance program?

A. Establishment of accountability
B. Compliance with audit requirements
C. Monitoring of security incidents
D. Creation of tactical solutions

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 87
The **PRIMARY** purpose of aligning information security with corporate governance objectives is to:

A. build capabilities to improve security processes.
B. consistently manage significant areas of risk.
C. identify an organization's tolerance for risk.
D. re-align roles and responsibilities.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 88

Which of the following is the **BEST** way to integrate information security into corporate governance?

A. Engage external security consultants in security initiatives.
B. Conduct comprehensive information security management training for key stakeholders.
C. Ensure information security processes are part of the existing management processes.
D. Require periodic security risk assessments be performed.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 89

Which of the following is the **MOST** effective way of ensuring that business units comply with an information security governance framework?

A. Integrating security requirements with processes
B. Performing security assessments and gap analysis
C. Conducting a business impact analysis (BIA)
D. Conducting information security awareness training

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 90

Which of the following **BEST** demonstrates alignment between information security governance and corporate governance?

A. Average number of security incidents across business units
B. Security project justifications provided in terms of business value
C. Number of vulnerabilities identified for high-risk information assets
D. Mean time to resolution for enterprise-wide security incidents

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 91
The **MOST** important element in achieving executive commitment to an information security governance program is:

A. a defined security framework
B. identified business drivers
C. established security strategies
D. a process improvement model

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 92
After implementing an information security governance framework, which of the following would provide the **BEST** information to develop an information security project plan?

A. Risk heat map
B. Recent audit results
C. Balanced scorecard
D. Gap analysis

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 93

An information security manager's **PRIMARY** objective for presenting key risks to the board of directors is to:
A. meet information security compliance requirements.
B. ensure appropriate information security governance.
C. quantity reputational risks.
D. re-evaluate the risk appetite.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 94
When developing an information security governance framework, which of the following should be the **FIRST** activity?

A. Integrate security within the system's development life-cycle process.
B. Align the information security program with the organization's other risk and control activities.
C. Develop policies and procedures to support the framework.
D. Develop response measures to detect and ensure the closure of security breaches.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is the **MOST** effective way for senior management to support the integration of information security governance into corporate governance?

A. Develop the information security strategy based on the enterprise strategy.
B. Appoint a business manager as heard of information security.
C. Promote organization-wide information security awareness campaigns.
D. Establish a steering committee with representation from across the organization.

Correct Answer: A

Section: INFORMATION SECURITY GOVERNANCE
Explanation
Explanation/Reference:

QUESTION 96
Which of the following is a **PRIMARY** responsibility of the information security governance function?

A. Defining security strategies to support organizational programs
B. Ensuring adequate support for solutions using emerging technologies
C. Fostering a risk-aware culture to strengthen the information security program
D. Advising senior management on optimal levels of risk appetite and tolerance

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 97
Which of the following is the **MOST** important requirement for the successful implementation of security governance?

A. Implementing a security balanced scorecard
B. Performing an enterprise-wide risk assessment
C. Mapping to organizational strategies
D. Aligning to an international security framework

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is a **PRIMARY** responsibility of an information security governance committee?

A. Analyzing information security policy compliance reviews

B. Approving the purchase of information security technologies
C. Reviewing the information security strategy
D. Approving the information security awareness training strategy

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 99
The **BEST** way to encourage good security practices is to:

A. schedule periodic compliance audits.
B. discipline those who fail to comply with the security policy.
C. recognize appropriate security behavior by individuals.
D. publish the information security policy.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 100
Which of the following enables compliance with a nonrepudiation policy requirement for electronic transactions?

A. Digital certificates
B. Digital signatures
C. Encrypted passwords
D. One-time passwords

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 101

A new version of an information security regulation is published that requires an organization's compliance. The information security manager should **FIRST:**

A. perform an audit based on the new version of the regulation.
B. conduct a risk assessment to determine the risk of noncompliance.
C. conduct benchmarking against similar organizations.
D. perform a gap analysis against the new regulation.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 102

Which of the following **BEST** demonstrates that an organization supports information security governance?

A. Employees attend annual organization-wide security training.
B. Information security policies are readily available to employees.
C. The incident response plan is documented and tested regularly.
D. Information security steering committee meetings are held regularly.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 103

Which of the following is the **BEST** approach for an information security manager when developing new information security policies?

A. Create a stakeholder map.
B. Reference an industry standard.
C. Establish an information security governance committee.
D. Download a policy template.

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 104
When supporting a large corporation's board of directors in the development of governance, which of the following is the **PRIMARY** function of the information security manager?

A. Gaining commitment of senior management
B. Preparing the security budget
C. Providing advice and guidance
D. Developing a balanced scorecard

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 105
Which of the following would be **MOST** important to consider when implementing security settings for a new system?

A. Results from internal and external audits
B. Government regulations and related penalties
C. Business objectives and related IT risk
D. Industry best practices applicable to the business

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 106

Senior management commitment and support will **MOST** likely be offered when the value of information security governance is presented from a:

A. threat perspective.
B. compliance perspective.
C. risk perspective.
D. policy perspective.

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 107
Within a security governance framework, which of the following is the MOST important characteristic of the information security committee? The committee:

A. conducts frequent reviews of the security policy
B. has established relationships with external professionals
C. has a clearly defined charter and meeting protocols
D. includes a mix of members from all levels of management

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 108
To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

A. interview senior management
B. conduct a risk assessment
C. conduct a cost-benefit analysis
D. perform a gap analysis

Correct Answer: D

Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 109
Which of the following **MOST** effectively helps an organization to align information security governance with corporate governance?

A. Promoting security as enabler to achieve business objectives
B. Prioritizing security initiatives based on IT strategy
C. Adopting global security standards to achieve business goals
D. Developing security performance metrics

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 110
Which of the following is **MOST** helpful for aligning security operations with the IT governance framework?

A. Information security policy
B. Security risk assessment
C. Security operations program
D. Business impact analysis (BIA)

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 111

When trying to integrate information security across an organization, the **MOST** important goal for a governing body should be to ensure:

A. the resources used for information security projects are kept to a minimum.

B. information security is treated as a business critical issue.
C. funding is approved for requested information security projects.
D. periodic information security audits are conducted.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 112
Which of the following is **MOST** critical for an effective information security governance framework?

A. Board members are committed to the information security program.
B. Information security policies are reviewed on a regular basis.
C. The information security program is continually monitored.
D. The CIO is accountable for the information security program.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 113
Which of the following is **MOST** important when establishing a successful information security governance framework?

A. Selecting information security steering committee members
B. Developing an information security strategy
C. Determining balanced scorecard metrics for information security
D. Identifying information security risk scenarios

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:
QUESTION 114
An organization enacted several information security policies to satisfy regulatory requirements. Which of the following situations would **MOST** likely increase the probability of noncompliance to these requirements?

A. Inadequate buy-in from system owners to support the policies
B. Availability of security policy documents on a public website
C. Lack of training for end users on security policies
D. Lack of an information security governance framework

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 115
Which of the following should be the **PRIMARY** consideration when developing a security governance framework for an enterprise?

A. Understanding of the current business strategy
B. Assessment of the current security architecture
C. Results of a business impact analysis (BIA)
D. Benchmarking against industry best practice

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 116
Which of the following would **BEST** help an information security manager prioritize remediation activities to meet regulatory requirements?

A. A capability maturity model matrix
B. Annual loss expectancy (ALE) of noncompliance
C. Cost of associated controls
D. Alignment with the IT strategy

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 117
Which of the following is the **PRIMARY** reason an information security strategy should be deployed across an organization?

A. To ensure that the business complies with security regulations
B. To ensure that management's intent is reflected in security activities
C. To ensure that employees adhere to security standards
D. To ensure that security-related industry best practices are adopted

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 118
Which of the following should an information security manager do **FIRST** after learning about a new regulation that affects the organization?

A. Evaluate the changes with legal counsel.
B. Notify the affected business units.
C. Assess the noncompliance risk.
D. Inform senior management of the new regulation.

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 119
Which of the following is **MOST** important to consider when handling digital evidence during the forensics investigation of a cybercrime?

A. Business strategies
B. Industry best practices
C. Global standardsD. Local regulations

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 120
A legacy application does not comply with new regulatory requirements to encrypt sensitive data at rest, and remediating this issue would require significant investment. What should the information security manager do **FIRST**?

A. Investigate alternative options to remediate the noncompliance.
B. Assess the business impact to the organization.
C. Present the noncompliance risk to senior management.
D. Determine the cost to remediate the noncompliance.

Correct Answer: B
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 121
Which of the following is a **PRIMARY** responsibility of an information security steering committee?

A. Reviewing the information security strategy
B. Approving the information security awareness training strategy
C. Analyzing information security policy compliance reviews

D. Approving the purchase of information security technologies

Correct Answer: A
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 122
Which of the following would **BEST** enable integration of information security governance into corporate governance?

A. Ensuring appropriate business representation on the information security steering committee
B. Using a balanced scorecard to measure the performance of the information security strategy
C. Implementing IT governance, risk and compliance (IT GRC) dashboards
D. Having the CIO chair the information security steering committee

Correct Answer: C
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 123
Which of the following **BEST** enables effective information security governance?

A. Periodic vulnerability assessments
B. Established information security metrics
C. Advanced security technologies
D. Security-aware corporate culture

Correct Answer: D
Section: INFORMATION SECURITY GOVERNANCE
Explanation

Explanation/Reference:

QUESTION 124
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: INFORMATION RISK MANAGEMENT
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.

QUESTION 125
Information security managers should use risk assessment techniques to:

A. justify selection of risk mitigation strategies.
B. maximize the return on investment (ROD.
C. provide documentation for auditors and regulators.
D. quantify risks that would otherwise be subjective.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

QUESTION 126

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: INFORMATION RISK MANAGEMENT
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 127
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: INFORMATION RISK MANAGEMENT
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 128
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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 129
The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 130
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

A. map the major threats to business objectives.
B. review available sources of risk information.
C. identify the value of the critical assets.
D. determine the financial impact if threats materialize.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 131
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: INFORMATION RISK MANAGEMENT
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 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 132
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: INFORMATION RISK MANAGEMENT
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 133
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Assets must be inventoried before any of the other choices can be performed.

QUESTION 134
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: INFORMATION RISK MANAGEMENT
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 135
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: INFORMATION RISK MANAGEMENT
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 136
The security responsibility of data custodians in an organization will include:

A. assuming overall protection of information assets.
B. determining data classification levels.
C. implementing security controls in products they install. D. ensuring security measures are consistent with policy.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 137
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: INFORMATION RISK MANAGEMENT
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 138
Which of the following risks is represented in the risk appetite of an organization?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 139
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: INFORMATION RISK MANAGEMENT
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 140
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: INFORMATION RISK MANAGEMENT
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.

QUESTION 141
Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 142
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: INFORMATION RISK MANAGEMENT
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 143
Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

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

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 144
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: INFORMATION RISK MANAGEMENT
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 145
Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
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 146
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: INFORMATION RISK MANAGEMENT
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 147
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 148
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: INFORMATION RISK MANAGEMENT
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 149
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: INFORMATION RISK MANAGEMENT
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 150
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its 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.

QUESTION 151

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: INFORMATION RISK MANAGEMENT
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 152
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: INFORMATION RISK MANAGEMENT
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

QUESTION 153
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:
Explanation:

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

QUESTION 154
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: INFORMATION RISK MANAGEMENT
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 155
Which program element should be implemented FIRST in asset classification and control?

A. Risk assessment

B. Classification
C. Valuation
D. Risk mitigation

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 156
When performing a risk assessment, the MOST important consideration is that:

A. management supports risk mitigation efforts.
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: INFORMATION RISK MANAGEMENT
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 157
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: INFORMATION RISK MANAGEMENT
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 158
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.
B. Perform a gap analysis.
C. Implement compensating controls.
D. Demand immediate compliance.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
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 159
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: INFORMATION RISK MANAGEMENT
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 160
Who is responsible for ensuring that information is classified?

A. Senior management
B. Security manager
C. Data owner
D. Custodian

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

QUESTION 161
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: INFORMATION RISK MANAGEMENT
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 162
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: INFORMATION RISK MANAGEMENT
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 163
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: INFORMATION RISK MANAGEMENT
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.

QUESTION 164
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: INFORMATION RISK MANAGEMENT
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 CIO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

QUESTION 165
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

A. develop an operational plan for achieving compliance with the 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: INFORMATION RISK MANAGEMENT
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 166
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: INFORMATION RISK MANAGEMENT
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 167
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 168
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: INFORMATION RISK MANAGEMENT
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 169
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: INFORMATION RISK MANAGEMENT
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 170
When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

A. Estimated productivity losses
B. Possible scenarios with threats and impacts
C. Value of information assets
D. Vulnerability assessment

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

QUESTION 171
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: INFORMATION RISK MANAGEMENT
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 172
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: INFORMATION RISK MANAGEMENT
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.

QUESTION 173
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: INFORMATION RISK MANAGEMENT
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 174

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: INFORMATION RISK MANAGEMENT
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 175
To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

A. Conducting a qualitative and quantitative risk 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: INFORMATION RISK MANAGEMENT
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 176

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: INFORMATION RISK MANAGEMENT
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 177
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: INFORMATION RISK MANAGEMENT
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 178
After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

A. Information security officer
B. Chief information officer (CIO)
C. Business owner
D. Chief executive officer (CFO)

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The business owner of the application needs to understand and accept the residual application risks.

QUESTION 179
The purpose of a corrective control is to:

A. reduce adverse events.
B. indicate compromise.
C. mitigate impact.
D. ensure compliance.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Corrective controls serve to reduce or mitigate impacts, such as providing recovery capabilities. Preventive controls reduce adverse events, such as firewalls. Compromise can be detected by detective controls, such as intrusion detection systems (IDSs). Compliance could be ensured by preventive controls, such as access controls.

QUESTION 180
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: INFORMATION RISK MANAGEMENT
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 181
It is MOST important for an information security manager to ensure that security risk assessments are performed:

A. consistently throughout the enterprise
B. during a root cause analysis
C. as part of the security business case
D. in response to the threat landscape

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Reference: https://m.isaca.org/Certification/Additional-Resources/Documents/CISM-Item-Development-Guide_bro_Eng_0117.pdf (14)

QUESTION 182
An information security manager has been asked to create a strategy to protect the organization's information from a variety of threat vectors. Which of the following should be done FIRST?

A. Perform a threat modeling exercise
B. Develop a risk profile
C. Design risk management processes
D. Select a governance framework

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 183
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

A. Integrating the risk assessment into the internal audit program
B. Applying global security standards to the IT projects
C. Training project managers on risk assessment
D. Having the information security manager participate on the project setting committees
Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 184
An information security manager has completed a risk assessment and has determined the residual risk. Which of the following should be the NEXT step?

A. Conduct an evaluation of controls
B. Determine if the risk is within the risk appetite
C. Implement countermeasures to mitigate risk
D. Classify all identified risks

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 185
Which of the following would be the BEST indicator that an organization is appropriately managing risk?

A. The number of security incident events reported by staff has increased

B. Risk assessment results are within tolerance
C. A penetration test does not identify any high-risk system vulnerabilities
D. The number of events reported from the intrusion detection system has declined

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 186
Which of the following vulnerabilities presents the GREATEST risk of external hackers gaining access to the corporate network?
A. Internal hosts running unnecessary services
B. Inadequate logging
C. Excessive administrative rights to an internal database
D. Missing patches on a workstation

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 187
When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

A. monitor for business changes
B. review the residual risk level
C. report compliance to management
D. implement controls to mitigate the risk

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 188
Which of the following would be MOST useful in a report to senior management for evaluating changes in the organization's information security risk position?

A. Risk register
B. Trend analysis
C. Industry benchmarks
D. Management action plan

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 189
An information security manager is preparing a presentation to obtain support for a security initiative. Which of the following would be the BEST way to obtain management's commitment for the initiative?

A. Include historical data of reported incidents
B. Provide the estimated return on investment
C. Provide an analysis of current risk exposures
D. Include industry benchmarking comparisons

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 190
Which of the following is the MOST significant security risk in IT asset management?

A. IT assets may be used by staff for private purposes
B. Unregistered IT assets may not be supported
C. Unregistered IT assets may not be included in security documentation
D. Unregistered IT assets may not be configured properly

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 191
Which of the following is the MOST effective method of preventing deliberate internal security breaches?

A. Screening prospective employees
B. Well-designed firewall system
C. Well-designed intrusion detection system (IDS)
D. Biometric security access control

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Reference: https://www.techrepublic.com/article/strategies-for-preventing-internal-security-breaches-in-a-growing-business/

QUESTION 192
A business previously accepted the risk associated with a zero-day vulnerability. The same vulnerability was recently exploited in a high-profile attack on another organization in the same industry. Which of the following should be the information security manager's FIRST course of action?

A. Reassess the risk in terms of likelihood and impact
B. Develop best and worst case scenarios
C. Report the breach of the other organization to senior management
D. Evaluate the cost of remediating the vulnerability

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 193
To effectively manage an organization's information security risk, it is MOST important to:

A. periodically identify and correct new systems vulnerabilities
B. assign risk management responsibility to end users
C. benchmark risk scenarios against peer organizations
D. establish and communicate risk tolerance

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 194
Which of the following is the BEST course of action for the information security manager when residual risk is above the acceptable level of risk?

A. Perform a cost-benefit analysis
B. Recommend additional controls
C. Carry out a risk assessment
D. Defer to business management

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 195
Which of the following is the BEST reason to initiate a reassessment of current risk?

A. Follow-up to an audit report
B. A recent security incident
C. Certification requirements
D. Changes to security personnel

Correct Answer: B

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 196
Before final acceptance of residual risk, what is the **BEST** way for an information security manager to address risk factors determined to be lower than acceptable risk levels?

A. Evaluate whether an excessive level of control is being applied.
B. Ask senior management to increase the acceptable risk levels.
C. Implement more stringent countermeasures.
D. Ask senior management to lower the acceptable risk levels.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 197
Which of the following is the **MOST** appropriate course of action when the risk occurrence rate is low but the impact is high?

A. Risk transfer
B. Risk acceptance
C. Risk mitigation
D. Risk avoidance

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 198
Which of the following is the **MOST** effective way to communicate information security risk to senior management?

A. Business impact analysis
B. Balanced scorecard
C. Key performance indicators (KPIs)
D. Heat map

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 199
Security risk assessments should cover only information assets that:

A. are classified and labeled.
B. are inside the organization.
C. support business processes.
D. have tangible value.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 200
Which of the following is an indicator of improvement in the ability to identify security risks?

A. Increased number of reported security incidents.
B. Decreased number of staff requiring information security training.
C. Decreased number of information security risk assessments.
D. Increased number of security audit issues resolved.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 201

Which of the following is the **MOST** important step in risk ranking?

A. Impact assessment
B. Mitigation cost
C. Threat assessment
D. Vulnerability analysis

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 202

Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:

A. inform senior management
B. update the risk assessment
C. validate the user acceptance testing
D. modify key risk indicators

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 203

Which of the following would BEST mitigate identified vulnerabilities in a timely manner?

A. Continuous vulnerability monitoring tool
B. Categorization of the vulnerabilities based on system's criticality
C. Monitoring of key risk indicators (KRIs)
D. Action plan with responsibilities and deadlines

Correct Answer: C

Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanations
One approach seeing increasing use is to report and monitor risk through the use of key risk indicators (KRIs). KRIs can be defined as measures that, in some manner, indicate when an enterprise is subject to risk that exceeds a defined risk level. Typically, these indicators are trends in factors known to increase risk and are generally developed based on experience. They can be as diverse as increasing absenteeism or increased turnover in key employees to rising levels of security events or incidents.

QUESTION 204
Risk assessment should be conducted on a continuing basis because:

A. controls change on a continuing basis
B. the number of hacking incidents is increasing
C. management should be updated about changes in risk
D. factors that affect information security change

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 205
Which of the following BEST illustrates residual risk within an organization?

A. Risk management framework
B. Risk register
C. Business impact analysis
D. Heat map

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 206
Which of the following is the **PRIMARY** goal of a risk management program?

A. Implement preventive controls against threats.
B. Manage the business impact of inherent risks.
C. Manage compliance with organizational policies.
D. Reduce the organization's risk appetite.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 207
The objective of risk management is to reduce risk to the minimum level that is:

A. compliant with security policies
B. practical given industry and regulatory environments. C. achievable from technical and financial perspectives.
D. acceptable given the preference of the organization.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 208
Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager's most important action is to:

A. provide senior management with risk treatment options.
B. design and implement controls to reduce the risk.
C. consult external third parties on how to treat the risk.
D. ensure that employees are aware of the risk.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 209
Which of the following is the **PRIMARY** reason for performing an analysis of the threat landscape on a regular basis?
A. To determine the basis for proposing an increase in security budgets.
B. To determine if existing business continuity plans are adequate.
C. To determine if existing vulnerabilities present a risk.
D. To determine critical information for executive management.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 210
Mitigating technology risks to acceptable levels should be based **PRIMARILY** upon:

A. business process reengineering.
B. business process requirement.
C. legal and regulatory requirements.
D. information security budget.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 211
After assessing risk, the decision to treat the risk should be based **PRIMARILY** on:

A. availability of financial resources.
B. whether the level of risk exceeds risk appetite.
C. whether the level of risk exceeds inherent risk.
D. the criticality of the risk.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 212
When preventative controls to appropriately mitigate risk are not feasible, which of the following is the **MOST** important action for the information security manager to perform?

A. Assess vulnerabilities.
B. Manage the impact.
C. Evaluate potential threats.
D. Identify unacceptable risk levels.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 213
Which of the following is the **GREATEST** risk of single sign-on?

A. It is a single point of failure for an enterprise access control process.
B. Password carelessness by one user may render the entire infrastructure vulnerable.
C. Integration of single sign-on with the rest of the infrastructure is complicated.
D. One administrator maintains the single sign-on solutions without segregation of duty.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 214
Deciding the level of protection a particular asset should be given in **BEST** determined by:

A. a threat assessment.

B. a vulnerability assessment.
C. a risk analysis.
D. the corporate risk appetite.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 215
Which of the following is the **BEST** method for determining whether new risks exist in legacy applications?

A. Regularly scheduled risk assessments
B. Automated vulnerability scans
C. Third-party penetration testing
D. Frequent updates to the risk register

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 216
Which of the following processes can be used to remediate identified technical vulnerabilities?

A. Running baseline configurations

B. Conducting a risk assessment
C. Performing a business impact analysis (BIA)
D. Running automated scanners

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 217
Which of the following would provide senior management with the **BEST** information to better understand the organization's information security risk profile?

A. Scenarios that impact business operations
B. Scenarios that disrupt client services
C. Scenarios that impact business goals
D. Scenarios that have a monetary impact

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 218
A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems, following should be the information security manager's PRIMARY concern?

A. Business tolerance of downtime
B. Adequacy of the incident response plan
C. Availability of resources to implement controls
D. Ability to test patches prior to deployment

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 219
Which of the following is the **MOST** important action when using a web application that has recognized vulnerabilities?

A. Deploy an application firewall.
B. Deploy host-based intrusion detection.
C. Install anti-spyware software.
D. Monitor application level logs.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 220
Which of the following is the **BEST** indicator of a successful external intrusion into computer systems?

A. Unexpected use of protocols within the DMZ.
B. Unexpected increase of malformed URLs.
C. Decrease in the number of login failures.
D. Spikes in the number of login failures.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 221
The likelihood of a successful attack is a function of:

A. incentive and capability of the intruder
B. opportunity and asset value
C. threat and vulnerability levels
D. value and desirability to the intruder

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 222
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: INFORMATION RISK MANAGEMENT
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 probability of the risk.

QUESTION 223
Which of the following BEST indicates a successful risk management practice?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 224
Which of the following will BEST protect an organization from internal security attacks?
A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employee awareness certification program

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
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 225
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: INFORMATION RISK MANAGEMENT
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 226
In a business impact analysis, the value of an information system should be based on the overall cost:
A. of recovery.
B. to recreate.
C. if unavailable.
D. of emergency operations.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 227
The value of information assets is BEST determined by:

A. individual business managers.
B. business systems analysts.
C. information security management.
D. industry averages benchmarking.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 228
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

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

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

QUESTION 229
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: INFORMATION RISK MANAGEMENT
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 230
The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

A. Mitigating controls
B. Visibility of impact
C. Likelihood of occurrence
D. Incident frequency
Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

QUESTION 231
Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. EvaluationD. Monitoring

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
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 232

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: INFORMATION RISK MANAGEMENT
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 233
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

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

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
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 234
Which of the following will BEST prevent external security attacks?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 235
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 236
A business impact analysis (BIA) is the BEST tool for calculating:

A. total cost of ownership.

B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:
A business impact analysis (BIA) is the best tool for calculating the priority of restoration for applications. It is not used to determine total cost of ownership, annualized loss expectancy (ALE) or residual risk to the organization.

QUESTION 237
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: INFORMATION RISK MANAGEMENT
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.

QUESTION 238
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: INFORMATION RISK MANAGEMENT
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 239
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: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

QUESTION 240
Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

A. Systems operation procedures are not enforced
B. Change management procedures are poor
C. Systems development is outsourced
D. Systems capacity management is not performed

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed by third-party vendors are becoming commonplace and do not represent an increase in security risk as much as poor change management. Poor capacity management may not necessarily represent a security risk.

QUESTION 241
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: INFORMATION RISK MANAGEMENT
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 242
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: INFORMATION RISK MANAGEMENT
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 243
An organization's recent risk assessment has identified many areas of security risk, and senior management has asked for a five-minute overview of the assessment results. Which of the following is the information security manager's **BEST** option for presenting this information?
A. Risk register
B. Risk heat map
C. Spider diagram
D. Balanced scorecard

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 244
Which of the following should be of **GREATEST** concern to an information security manager when establishing a set of key risk indicators (KRIs)?

A. The impact of security risk on organizational objectives is not well understood.
B. Risk tolerance levels have not yet been established.
C. Several business functions have been outsourced to third-party vendors.
D. The organization has no historical data on previous security events.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 245
When management changes the enterprise business strategy, which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?

A. Risk management
B. Change management
C. Access control management
D. Configuration management

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 246
What is the **PRIMARY** benefit to executive management when audit, risk, and security functions are aligned?

A. Reduced number of assurance reports
B. More effective decision making C. More timely risk reporting
D. More efficient incident handling

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 247
A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should **FIRST**:

A. evaluate a third-party solution.
B. deploy additional security controls.
C. evaluate the business risk.
D. initiate an exception approval process.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 248
Which of the following is **MOST** helpful for prioritizing the recovery of IT assets during a disaster?

A. Business impact analysis (BIA)
B. Risk assessment
C. Vulnerability assessment
D. Cost-benefit analysis

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 249
Risk management is **MOST** cost-effective:

A. when performed on a continuous basis.
B. while developing the business case for the security program.
C. at the beginning of security program development.
D. when integrated into other corporate assurance functions.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 250
The **MOST** effective way to communicate the level of impact of information security risks on organizational objectives is to present:

A. business impact analysis (BIA) results.
B. detailed threat analysis results.

C. risk treatment options.
D. a risk heat map.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 251
Senior management has decided to accept a significant risk within a security remediation plan.

Which of the following is the information security manager's **BEST** course of action?

A. Remediate the risk and document the rationale.
B. Update the risk register with the risk acceptance.
C. Communicate the remediation plan to the board of directors.
D. Report the risk acceptance to regulatory agencies.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 252
Which of the following is **MOST** important to consider when prioritizing threats during the risk assessment process?

A. The criticality of threatened systems
B. The severity of exploited vulnerabilities
C. The potential impact on operations
D. The capability of threat actors

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 253
Which of the following is the **BEST** control to minimize the risk associated with loss of information as a result of ransomware exploiting a zero-day vulnerability?

A. A security operation center
B. A patch management process
C. A public key infrastructure
D. A data recovery process

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 254
A **PRIMARY** advantage of involving business management in evaluating and managing information security risks is that they:

A. better understand organizational risks.
B. can balance technical and business risks.
C. are more objective than security management.
D. better understand the security architecture.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 255
In addition to cost, what is the **BEST** criteria for selecting countermeasures following a risk assessment?

A. Effort of implementation
B. Skill requirements for implementation
C. Effectiveness of each option
D. Maintenance requirements

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 256
Vulnerability scanning has detected a critical risk in a vital business application. Which of the following should the information security manager do **FIRST**?

A. Report the business risk to senior management.
B. Confirm the risk with the business owner.
C. Update the risk register.
D. Create an emergency change request.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 257
A risk was identified during a risk assessment. The business process owner has chosen to accept the risk because the cost of remediation is greater than the projected cost of a worst-case scenario. What should be the information security manager's **NEXT** course of action?

A. Determine a lower-cost approach to remediation.
B. Document and schedule a date to revisit the issue.
C. Shut down the business application.
D. Document and escalate to senior management.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 258
An inexperienced information security manager is relying on its internal audit department to design and implement key security controls. Which of the following is the **GREATEST** risk?

A. Inadequate implementation of controls
B. Conflict of interest
C. Violation of the audit charter
D. Inadequate audit skills

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 259
The **MOST** likely reason to use qualitative security risk assessments instead of quantitative methods is when:

A. an organization provides services instead of hard goods.
B. a security program requires independent expression of risks.
C. available data is too subjective.
D. a mature security program is in place.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 260
The **PRIMARY** objective of a risk response strategy should be:

A. threat reduction.
B. regulatory compliance.
C. senior management buy-in.
D. appropriate control selection.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 261
An organization has concerns regarding a potential advanced persistent threat (APT). To ensure that the risk associated with this threat is appropriately managed, what should be the organization's **FIRST** action?

A. Report to senior management.
B. Initiate incident response processes.
C. Implement additional controls.
D. Conduct an impact analysis.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 262
An organization plans to implement a document collaboration solution to allow employees to share company information. Which of the following is the **MOST** important control to mitigate the risk associated with the new solution?

A. Assign write access to data owners.
B. Allow a minimum number of user access to the solution.
C. Have data owners perform regular user access reviews.
D. Permit only non-sensitive information on the solution.

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 263
Which of the following is the **MOST** important function of information security?

A. Managing risk to the organization

B. Reducing the financial impact of security breaches
C. Identifying system vulnerabilities
D. Preventing security incidents
Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 264
Which of the following **BEST** describes a buffer overflow?

A. A program contains a hidden and unintended function that presents a security risk.
B. A type of covert channel that captures data.
C. Malicious code designed to interfere with normal operations.
D. A function is carried out with more data than the function can handle.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 265
Which of the following **BEST** protects against web-based cross-domain attacks?

A. Database hardening
B. Application controls
C. Network addressing scheme
D. Encryption controls

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 266
Which of the following would be **MOST** effective in preventing malware from being launched through an email attachment?
A. Up-to-date security policies
B. Placing the e-mail server on a screened subnet
C. Security awareness training
D. A network intrusion detection system (NIDS)

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 267
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
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 268
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: INFORMATION RISK MANAGEMENT
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 269
Which of the following is the MOST usable deliverable of an information security risk analysis?

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

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 270
Information security policies should be designed **PRIMARILY** on the basis of:

A. business demands.
B. inherent risks
C. international standards.
D. business risks.

Correct Answer: D

Section: INFORMATION RISK MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 271
Which of the following should be the **PRIMARY** basis for determining risk appetite?

A. Organizational objectives
B. Senior management input
C. Industry benchmarks
D. Independent audit results

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 272
When scoping a risk assessment, assets need to be classified by:

A. likelihood and impact.
B. sensitivity and criticality.
C. threats and opportunities.
D. redundancy and recoverability.

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 273
Which is the **BEST** way for an organization to monitor security risk?

A. Analyzing key performance indicators (KPIs)

B. Using external risk intelligence services
C. Using a dashboard to assess vulnerabilities
D. Analyzing key risk indicators (KRIs)

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 274
An awareness program is implemented to mitigate the risk of infections introduced through the use of social media. Which of the following will **BEST** determine the effectiveness of the awareness program?

A. A post-awareness program survey
B. A quiz based on the awareness program materials
C. A simulated social engineering attack
D. Employee attendance rate at the awareness program

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 275
Which of the following is **MOST** important to consider when defining control objectives?

A. The current level of residual risk
B. The organization's strategic objectives
C. Control recommendations from a recent audit
D. The organization's risk appetite

Correct Answer: B
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 276

Which of the following should be the **MOST** important consideration when reporting sensitive risk-related information to stakeholders?

A. Ensuring nonrepudiation of communication
B. Consulting with the public relations director
C. Transmitting the internal communication securely
D. Customizing the communication to the audience

Correct Answer: C
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 277

Conflicting objectives are **MOST** likely to compromise the effectiveness of the information security process when information security management is:

A. reporting to the network infrastructure manager.
B. outside of information technology.
C. partially staffed by external security consultants.
D. combined with the change management function.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 278

Which of the following is **MOST** important for an information security manager to ensure when evaluating change requests?

A. Requests are approved by process owners.
B. Requests add value to the business.
C. Residual risk is within risk tolerance.
D. Contingency plans have been created.

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 279
Which of the following trends would be of **GREATEST** concern when reviewing the performance of an organization's intrusion detection systems (IDS)?

A. Decrease in false negatives
B. Increase in false positives
C. Decrease in false positives
D. Increase in false negatives

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 280
Shortly after installation, an intrusion detection system (IDS) reports a violation. Which of the following is the **MOST** likely explanation?

A. The violation is a false positive.
B. A routine IDS log file upload has occurred.
C. A routine IDS signature file download has occurred.
D. An intrusion has occurred.

Correct Answer: A
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 281
Which of the following provides the **GREATEST** assurance that information security is addressed in change management?

A. Performing a security audit on changes
B. Providing security training for change advisory board
C. Requiring senior management sign-off on change management
D. Reviewing changes from a security perspective

Correct Answer: D
Section: INFORMATION RISK MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 282
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. ensure the confidentiality of sensitive material.
B. provide a high assurance of identity.
C. allow deployment of the active directory.
D. implement secure sockets layer (SSL) encryption.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 283
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 284
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 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 285
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 286
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. messages displayed at every logon.
B. periodic security-related e-mail messages.
C. an Intranet web site for information security.
D. circulating the information security policy.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 287
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 288
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 289
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

A. to a higher false reject rate (FRR).
B. to a lower crossover error rate.
C. to a higher false acceptance rate (FAR).
D. exactly to the crossover error rate.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary' to reduce sensitivity and thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts — the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

QUESTION 290
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 291
An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross training. Which type of authorization policy would BEST address this practice?

A. Multilevel
B. Role-based
C. Discretionary
D. Attribute-based

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

A role-based policy will associate data access with the role performed by an individual, thus restricting access to data required to perform the individual's tasks. Multilevel policies are based on classifications and clearances. Discretionary policies leave access decisions up to information resource managers.

QUESTION 292
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 293
Which of the following guarantees that data in a file have not changed?

A. Inspecting the modified date of the file
B. Encrypting the file with symmetric encryption
C. Using stringent access control to prevent unauthorized access
D. Creating a hash of the file, then comparing the file hashes

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:
Explanation:

A hashing algorithm can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

QUESTION 294
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 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 295
Nonrepudiation can BEST be ensured by using:

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

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
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.

QUESTION 296
The implementation of a capacity plan would prevent:

A. file system overload arising from distributed denial-of-service attacks
B. system downtime for scheduled security maintenance
C. software failures arising from exploitation of buffer capacity vulnerabilities
D. application failures arising from insufficient hardware resources

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 297
An organization plans to allow employees to use their own devices on the organization’s network. Which of the following is the information security manager’s BEST course of action?

A. Implement automated software
B. Assess associated risk
C. Conduct awareness training
D. Update the security policy

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 298
When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:
A. give the business a measure of the organization's overall readiness
B. provide participants with situations to ensure understanding of their roles
C. measure management engagement as part of an incident response team
D. challenge the incident response team to solve the problem under pressure

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanations
Tabletop scenarios that need to be completed with one hour per scenario using full escalation as per decision trees to accurately simulate and evaluate responses of each team member and the processes within the playbooks.

QUESTION 299
Which of the following is the PRIMARY advantage of desk checking a business continuity plan (BCP)?

A. Assesses the availability and compatibility a backup hardware
B. Allows for greater participation be management and the IT department
C. Ensures that appropriate follow-up work is performed on noted issues
D. Provides a low-cost method of assessing the BCP's completeness

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 300
When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the **BEST** method to determine the priority of system recovery in the event of a disaster?

A. Evaluating the cost associated with each system's outage

B. Reviewing the business plans of each department
C. Comparing the recovery point objectives (RPOs)
D. Reviewing each system's key performance indicators (KPIs)
Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 301
Information security awareness programs are **MOST** effective when they are:

A. customized for each target audience.
B. sponsored by senior management.
C. reinforced by computer-based training.
D. conducted at employee orientation

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 302
Which of the following is the **MOST** effective method of determining security priorities?

A. Impact analysis
B. Threat assessment
C. Vulnerability assessment
D. Gap analysis

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 303
To implement a security framework, an information security manager must **FIRST** develop:
A. security standards.
B. security procedures.
C. a security policy.
D. security guidelines.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 304
An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

A. document and report the root cause of the incidents for senior management.
B. identify security program gaps or systemic weaknesses that need correction.
C. prepare properly vetted notifications regarding the incidents to external parties.
D. identify who should be held accountable for the security incidents.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 305
An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions in-house. The information security manager has determined a defense in depth strategy should be used. Which of the following **BEST** describes this strategy?

A. Multi-factor login requirements for cloud service applications, timeouts, and complex passwords
B. Deployment of nested firewalls within the infrastructure
C. Separate security controls for applications, platforms, programs, and endpoints

D. Strict enforcement of role-based access control (RBAC)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 306
When supporting an organization's privacy officer, which of the following is the information security manager's **PRIMARY** role regarding primacy requirements?

A. Monitoring the transfer of private data
B. Conducting privacy awareness programs
C. Ensuring appropriate controls are in place
D. Determining data classification

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 307
Which of the following metrics would provide management with the **MOST** useful information about the progress of a security awareness program?

A. Increased number of downloads of the organization's security policy
B. Increased reported of security incidents
C. Completion rate of user awareness training within each business unit
D. Decreased number of security incidents

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 308
An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's **FIRST** step to support this strategy?

A. Incorporate social media into the security awareness program.
B. Develop a guideline on the acceptable use of social media.
C. Develop a business case for a data loss prevention (DLP) solution.
D. Employ the use of a web content filtering solution.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 309
Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. End users
B. Corporate auditors
C. Process owners
D. Security architects

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 310
An information security manager is developing a business case for an investment in an information security control. The FIRST step should be to:

A. research vendor pricing to show cost efficiency
B. assess potential impact to the organization
C. demonstrate increased productivity of security staff
D. gain audit buy-in for the security control

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:

QUESTION 311
The contribution of recovery point objective (RPO) to disaster recovery is to:

A. define backup strategy.
B. eliminate single points of failure.
C. reduce mean time between failures (MTBF).
D. minimize outage period.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 312
Which metric is the **BEST** indicator that an update to an organization's information security awareness strategy is effective?

A. A decrease in the number of incidents reported by staff
B. A decrease in the number of email viruses detected
C. An increase in the number of email viruses detected
D. An increase in the number of incidents reported by staff

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 313
An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:

A. risk assessment results.
B. international security standards.
C. the most stringent requirements.
D. the security organization structure.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 314
Which if the following would be the **MOST** important information to include in a business case for an information security project in a highly regulated industry?

A. Compliance risk assessment
B. Critical audit findings
C. Industry comparison analysis
D. Number of reported security incidents

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 315
Which of the following should be of **MOST** concern to an information security manager reviewing an organization's data classification program?

A. The program allows exceptions to be granted.
B. Labeling is not consistent throughout the organization.
C. Data retention requirement are not defined.
D. The classifications do not follow industry best practices.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 316

Which of the following would the **BEST** demonstrate the added value of an information security program?

A. Security baselines
B. A SWOT analysis
C. A gap analysis
D. A balanced scorecard

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 317

Which of the following should be **PRIMARILY** included in a security training program for business process owners?

A. Impact of security risks
B. Application vulnerabilities
C. Application recovery time
D. List of security incidents reported

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 318

A CIO has asked the organization's information security manager to provide both one-year and five-year plans for the information security program. What is the **PRIMARY** purpose for the long-term plan?

A. To create formal requirements to meet projected security needs for the future
B. To create and document a consistent progression of security capabilities
C. To prioritize risks on a longer scale than the one-year plan

D. To facilitate the continuous improvement of the IT organization
Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 319
Which of the following has the **MOST** direct impact on the usability of an organization's asset classification program?

A. The granularity of classifications in the hierarchy
B. The frequency of updates to the organization's risk register
C. The business objectives of the organization
D. The support of senior management for the classification scheme

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 320
Which of the following is the MOST important factor to ensure information security is meeting the organization's objectives?

A. Internal audit's involvement in the security process
B. Implementation of a control self-assessment process
C. Establishment of acceptable risk thresholds
D. Implementation of a security awareness program

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 321

An organization has an approved bring your own device (BYOD) program. Which of the following is the **MOST** effective method to enforce application control on personal devices?

A. Establish a mobile device acceptable use policy.
B. Implement a mobile device management solution.
C. Educate users regarding the use of approved applications.
D. Implement a web application firewall.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 322
Which of the following is the **GREATEST** benefit of integrating information security program requirements into vendor management?

A. The ability to reduce risk in the supply chain
B. The ability to meet industry compliance requirements
C. The ability to define service level agreements (SLAs)
D. The ability to improve vendor performance

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 323
Which of the following is a step in establishing a security policy?

A. Developing platform-level security baselines
B. Creating a RACI matrix
C. Implementing a process for developing and maintaining the policy
D. Developing configuration parameters for the network

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 324
The **BEST** time to ensure that a corporation acquires secure software products when outsourcing software development is during:

A. corporate security reviews.
B. contract performance audits.
C. contract negotiation.
D. security policy development.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 325
An organization with a strict need-to-know information access policy is about to launch a knowledge management intranet.

Which of the following is the **MOST** important activity to ensure compliance with existing security policies?

A. Develop a control procedure to check content before it is published.
B. Change organization policy to allow wider use of the new web site.
C. Ensure that access to the web site is limited to senior managers and the board.
D. Password-protect documents that contain confidential information.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 326
Which of the following if the MOST significant advantage of developing a well-defined information security strategy?

A.

Support for buy-in from organizational employees
B. Allocation of resources to highest priorities
C. Prevention of deviations from risk tolerance thresholds
D. Increased maturity of incident response processes

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 327
Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?

A. The indicator should possess a high correlation with a specific risk and be measured on a regular basis.
B. The indicator should focus on IT and accurately represent risk variances.
C. The indicator should align with key performance indicators and measure root causes of process performance issues.
D. The indicator should provide a retrospective view of risk impacts and be measured annually.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 328
When implementing security architecture, an information security manager **MUST** ensure that security controls:

A. form multiple barriers against threats.
B. are transparent.
C. are the least expensive.
D. are communicated through security policies.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 329
An information security manager is reviewing the business case for a security project that is entering the development phase. It is determined that the estimated cost of the controls is now greater than the risk being mitigated.

The information security manager's **BEST** recommendation would be to:

A. eliminate some of the controls from the project scope.
B. discontinue the project to release funds for other efforts.
C. pursue the project until the benefits cover the costs.
D. slow the pace of the project to spread costs over a longer period.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 330
An organization is developing a disaster recovery plan for a data center that hosts multiple applications. The application recovery sequence would **BEST** be determined through an analysis of:

A. Key performance indicators (KPIs)
B. Recovery time objectives (RTOs)
C. Recovery point objectives (RPOs)
D. The data classification scheme

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 331

A.

Which of the following should be the **PRIMARY** goal of an information security manager when designing information security policies?
Reducing organizational security risk
B. Improving the protection of information
C. Minimizing the cost of security controls
D. Achieving organizational objectives

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 332
When developing a disaster recovery plan, which of the following would be **MOST** helpful in prioritizing the order in which systems should be recovered?

A. Performing a business impact analysis (BIA)
B. Measuring the volume of data in each system
C. Reviewing the information security policy
D. Reviewing the business strategy

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 333
Which of the following is the **PRIMARY** responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Require remote wipe capabilities for devices.
B. Enforce passwords and data encryption on the devices.
C. Conduct security awareness training.
D. Review and update existing security policies.

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:

QUESTION 334
Which of the following should be the **PRIMARY** consideration when selecting a recovery site?

A. Regulatory requirements
B. Recovery time objective
C. Geographical location
D. Recovery point objective

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 335
Management has announced the acquisition of a new company. The information security manager of parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies.

To **BEST** address this concern, the information security manager should:

A. escalate concern for conflicting access rights to management.
B. implement consistent access control standards.
C. review access rights as the acquisition integration occurs.
D. perform a risk assessment of the access rights.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

A.

QUESTION 336
Which of the following is the **BEST** method to determine whether an information security program meets an organization's business objectives?
Implement performance measures.
B. Review against international security standards.
C. Perform a business impact analysis (BIA).
D. Conduct an annual enterprise-wide security evaluation.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 337
A **PRIMARY** purpose of creating security policies is to:

A. implement management's governance strategy.
B. establish the way security tasks should be executed.
C. communicate management's security expectations.
D. define allowable security boundaries.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 338
Which of the following should be the **PRIMARY** consideration for an information security manager when designing security controls for a newly acquired business application?

A. Known vulnerabilities in the application
B. The IT security architecture framework
C. Cost-benefit analysis of current controls
D. Business processes supported by the application

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation
Explanation/Reference:

QUESTION 339
Which of the following would provide the **BEST** justification for a new information security investment?

A. Results of a comprehensive threat analysis.
B. Projected reduction in risk.
C. Senior management involvement in project prioritization.
D. Defined key performance indicators (KPIs)

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 340
Which of the following is the **PRIMARY** reason for executive management to be involved in establishing an enterprise's security management framework?

A. To determine the desired state of enterprise security
B. To establish the minimum level of controls needed
C. To satisfy auditors' recommendations for enterprise security
D. To ensure industry best practices for enterprise security are followed

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 341

A.

Which of the following needs to be established between an IT service provider and its clients to the **BEST** enable adequate continuity of service in preparation for an outage?

A. Data retention policies

B. Server maintenance plans C. Recovery time objectives
D. Reciprocal site agreement

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 342
Threat and vulnerability assessments are important **PRIMARILY** because they are:

A. needed to estimate risk
B. the basis for setting control objectives
C. elements of the organization's security posture
D. used to establish security investments

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 343
Which of the following is the **PRIMARY** goal of business continuity management?

A. Establish incident response procedures.
B. Assess the impact to business processes.
C. Increase survivability of the organization.
D. Implement controls to prevent disaster.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 344
Which of the following should an information security manager establish **FIRST** to ensure security-related activities are adequately monitored?

A. Internal reporting channels
B. Accountability for security functions
C. Scheduled security assessments
D. Regular reviews of computer system logs

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 345
What is the role of the information security manager in finalizing contract negotiations with service providers?

A. To update security standards for the outsourced process
B. To ensure that clauses for periodic audits are included
C. To obtain a security standard certification from the provider
D. To perform a risk analysis on the outsourcing process

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 346
Which of the following would provide the MOST effective security outcome in an organization's contract management process?

A. Extending security assessment to include random penetration testing
B. Extending security assessment to cover asset disposal on contract termination
C. Performing vendor security benchmark analyses at the request-for-proposal stage
D. Ensuring security requirements are defined at the request-for-proposal stage

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 347
An organization's outsourced firewall was poorly configured and allowed unauthorized access that resulted in downtime of 48 hours. Which of the following should be the information security manager's **NEXT** course of action?

A. Reconfigure the firewall in accordance with best practices.
B. Obtain supporting evidence that the problem has been corrected.
C. Revisit the contract and improve accountability of the service provider.
D. Seek damages from the service provider.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 348
The **PRIMARY** advantage of involving end users in continuity planning is that they:

A. are more objective than information security management.
B. can balance the technical and business risks.
C. have a better understanding of specific business needs.
D. can see the overall impact to the business.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 349
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 350
The effectiveness of virus detection software is MOST dependent on which of the following?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 351
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 device.

QUESTION 352
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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.

QUESTION 353
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 354
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 355
Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

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

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 356
When contracting with an outsourcer to provide security administration, the MOST important 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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 357
A third-party service provider is developing a mobile app for an organization’s customers.

Which of the following issues should be of **GREATEST** concern to the information security manager?

A. Software escrow is not addressed in the contract.
B. The contract has no requirement for secure development practices.
C. The mobile app’s programmers are all offshore contractors.
D. SLAs after deployment are not clearly defined.

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 358
Implementing a strong password policy is part of an organization's information security strategy for the year. A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy.

Which of the following is the information security manager's **BEST** course of action?

A. Analyze the risk and impact of not implementing the policy.
B. Develop and implement a password policy for the mobile application.
C. Escalate non-implementation of the policy to senior management.
D. Benchmark with similar mobile applications to identify gaps.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 359
What is the **MOST** important consideration when establishing metrics for reporting to the information security strategy committee?

A. Agreeing on baseline values for the metrics
B. Developing a dashboard for communicating the metrics
C. Providing real-time insight on the security posture of the organization
D. Benchmarking the expected value of the metrics against industry standards

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 360
Which of the following is the **BEST** approach for encouraging business units to assume their roles and responsibilities in an information security program?

A. Perform a risk assessment.
B. Conduct an awareness program.
C. Conduct a security audit.
D. Develop controls and countermeasures.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 361
When developing a new application, which of the following is the **BEST** approach to ensure compliance with security requirements?

A. Provide security training for developers.
B. Prepare detailed acceptance criteria.
C. Adhere to change management processes.
D. Perform a security gap analysis.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 362
Which of the following will **BEST** help to ensure security is addressed when developing a custom application?

A. Conducting security training for the development staff
B. Integrating security requirements into the development process
C. Requiring a security assessment before implementation
D. Integrating a security audit throughout the development process

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 363
What should be the PRIMARY objective of conducting interviews with business unit managers when developing an information security strategy?

A. Determine information types
B. Obtain information on departmental goals
C. Identify data and system ownership
D. Classify information assets

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 364
Which of the following is MOST important to consider when developing a disaster recovery plan?

A. Business continuity plan (BCP)
B. Business impact analysis (BIA)
C. Cost-benefit analysis
D. Feasibility assessment

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 365
Which of the following is the MOST effective approach for integrating security into application development?

A. Defining security requirements
B. Performing vulnerability scans
C. Including security in user acceptance testing sign-off
D. Developing security models in parallel

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 366
Which of the following should be of MOST influence to an information security manager when developing IT security policies?

A. Past and current threats
B. IT security framework
C. Compliance with regulations
D. Business strategy

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 367
Which of the following contributes **MOST** to the effective implementation of an information security strategy?

A. Reporting of security metrics
B. Regular security awareness training
C. Endorsement by senior management
D. Implementation of security standards

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 368

Which of the following **BEST** validates that security controls are implemented in a new business process?

A. Assess the process according to information security policy.
B. Benchmark the process against industry practices.
C. Verify the use of a recognized control framework.
D. Review the process for conformance with information security best practices.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 369

When preparing a business case for the implementation of a security information and event management (SIEM) system, which of the following should be a

PRIMARY driver in the feasibility study?

A. Cost of software
B. Cost-benefit analysis
C. Implementation timeframe
D. Industry benchmarks

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 370

When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?

A. Retention
B. Tuning

C. Encryption
D. Report distribution

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 371
Which of the following is MOST critical to the successful implementation of information security within an organizational?

A. The information security manager is responsible for setting information security policy
B. Strong risk management skills exist within the information security group
C. Budget is allocated for information security tools
D. Security is effectively marketed to all managers and employees

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 372
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 373
Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 374
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: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 375
Who can BEST approve plans to implement an information security governance framework?
A. Internal auditor
B. Information security management
C. Steering committee
D. Infrastructure management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary' to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

QUESTION 376
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 377
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

QUESTION 378
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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.

QUESTION 379
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 380
An intranet server should generally be placed on the:

A. internal network.
B. firewall server.
C. external router.
D. primary domain controller.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary- domain controllers do not normally share the physical device as the intranet server.

QUESTION 381
Security awareness training is MOST likely to lead to which of the following?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 382
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 383
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: INFORMATION SECURITY PROGRAM DEVELOPMENT

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 384

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: INFORMATION SECURITY PROGRAM DEVELOPMENT

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 385

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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 386
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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 387
Which of the following is MOST important to the success of an information security program?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 388
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 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 389
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 390
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 391
What is an appropriate frequency for updating operating system (OS) patches on production servers?

A. During scheduled rollouts of new applications
B. According to a fixed security patch management schedule
C. Concurrently with quarterly hardware maintenance
D. Whenever important security patches are released

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Patches should be applied whenever important security updates are released. They should not be delayed to coincide with other scheduled rollouts or maintenance. Due to the possibility of creating a system outage, they should not be deployed during critical periods of application activity such as month-end or quarter-end closing.

QUESTION 392
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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.

QUESTION 393
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 394
An e-commerce order fulfillment web server should generally be placed on which of the following?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 395
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 396
What is the BEST defense against a Structured Query Language (SQL) injection attack?

A. Regularly updated signature files
B. A properly configured firewall
C. An intrusion detection system
D. Strict controls on input fields

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Structured Query Language (SQL) injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent of fooling the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written; software is available to test for such weaknesses. All other choices would fail to prevent such an attack.

QUESTION 397
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 398
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager
B. Establish predetermined automatic expiration dates
C. Require managers to e-mail security when the user leaves
D. Ensure each individual has signed a security acknowledgement

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 399
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. corporate internal auditor.
B. System developers/analysts.
C. key business process owners.
D. corporate legal counsel.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 400
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 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 401
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 402
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 403
Which of the following is the MOST important risk associated with middleware in a client-server environment?

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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 404
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

A. Security in storage and transmission of sensitive data
B. Provider's level of compliance with industry standards
C. Security technologies in place at the facility
D. Results of the latest independent security review

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

Mow the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

QUESTION 405
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 406

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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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.

QUESTION 407
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 protocol.

QUESTION 408
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 409
Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 410
What should the information security manager recommend to support the development of a new web application that will allow retail customers to view inventory and order products?
A. Building an access control matrix
B. Request customers adhere to baseline security standards
C. Access through a virtual private network (VPN)
D. Implementation of secure transmission protocols

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 411
After adopting an information security framework, an information security manager is working with senior management to change the organization-wide perception that information security is solely the responsibility of the information security department. To achieve this objective, what should be the information security manager's **FIRST** initiative?

A. Develop an operational plan providing best practices for information security projects.
B. Develop an information security awareness campaign with senior management's support.
C. Document and publish the responsibilities of the information security department.
D. Implement a formal process to conduct periodic compliance reviews.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 412
Which of the following should be an information security manager's **PRIMARY** focus during the development of a critical system storing highly confidential data?

A. Ensuring the amount of residual risk is acceptable

B. Reducing the number of vulnerabilities detected
C. Avoiding identified system threats
D. Complying with regulatory requirements

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 413
Which of the following is the **BEST** reason to develop comprehensive information security policies?

A. To comply with external industry and government regulations
B. To support development of effective risk indicators
C. To align the information security program to organizational strategy
D. To gain senior management support for the information security program

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 414
An organization has announced new initiatives to establish a big data platform and develop mobile apps. What is the **FIRST** step when defining new human resource requirements?

A. Request additional funding for recruiting and training.
B. Analyze the skills necessary to support the new initiatives.
C. Benchmark to an industry peer.
D. Determine the security technology requirements for the initiatives.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 415
What is the **PRIMARY** role of the information security program?

A. To develop and enforce a set of security policies aligned with the business
B. To educate stakeholders regarding information security requirements
C. To perform periodic risk assessments and business impact analyses (BIAs)
D. To provide guidance in managing organizational security risk

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 416
An information security program should be established **PRIMARILY** on the basis of:

A. the approved information security strategy.
B. the approved risk management approach.
C. data security regulatory requirements.
D. senior management input.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 417
To ensure adequate disaster-preparedness among IT infrastructure personnel, it is **MOST** important to:

A. have the most experienced personnel participate in recovery tests.
B. include end-user personnel in each recovery test.

C. assign personnel-specific duties in the recovery plan.
D. periodically rotate recovery-test participants.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 418
In an organization implementing a data classification program, ultimate responsibility for the data on the database server lies with the:

A. information security manager
B. business unit manager.
C. database administrator (DBA).
D. information technology manager:

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 419
Which of the following is **MOST** important for an information security manager to consider when identifying information security resource requirements?

A. Information security incidents
B. Information security strategy
C. Current resourcing levels
D. Availability of potential resources

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 420
Which of the following is the **BEST** strategy to implement an effective operational security posture?

A. Threat management
B. Defense in depth
C. Increased security awareness
D. Vulnerability management
Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 421
What should be the **PRIMARY** basis for establishing a recovery time objective (RTO) for a critical business application?

A. Business impact analysis (BIA) results
B. Related business benchmarks
C. Risk assessment results
D. Legal and regulatory requirements

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 422
Which of the following **BEST** supports the alignment of information security with business functions?

A. Creation of a security steering committee
B. IT management support of security assessments
C. Business management participation in security penetration tests
D. A focus on technology security risk within business processes

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 423
Which of the following **MUST** be established before implementing a data loss prevention (DLP) system?
A. Privacy impact assessment
B. A data backup policy
C. Data classification
D. A data recovery policy

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 424
An IT department plans to migrate an application to the public cloud. Which of the following is the information security manager's **MOST** important action in support of this initiative?

A. Calculate security implementation costs.
B. Evaluate service level agreements (SLAs).
C. Provide cloud security requirements.
D. Review cloud provider independent assessment reports.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 425

Which of the following is the **MOST** effective way to ensure the process for granting access to new employees is standardized and meets organizational security requirements?

A. Grant authorization to individual systems as required with the approval of information security management.
B. Require managers of new hires be responsible for account setup and access during employee orientation.
C. Embed the authorization and creation of accounts with HR onboarding procedures.
D. Adopt a standard template of access levels for all employees to be enacted upon hiring.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 426
Which of the following has the **GREATEST** impact on efforts to improve an organization's security posture?

A. Supportive tone at the top management regarding security
B. Well-documented security policies and procedures
C. Regular reporting to senior management
D. Automation of security controls

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 427
Which if the following is **MOST** important to building an effective information security program?

A. Information security architecture to increase monitoring activities
B. Management support for information security
C. Relevant and timely content included in awareness programs
D. Logical access controls for information systems

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 428
Which of the following is the **BEST** way to address any gaps identified during an outsourced provider selection and contract negotiation process?

A. Make the provider accountable for security and compliance
B. Perform continuous gap assessments
C. Include audit rights in the service level agreement (SLA)
D. Implement compensating controls

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 429
Which of the following is the **BEST** course of action for an information security manager to align security and business goals?

A. Defining key performance indicators (KPIs)
B. Actively engaging with stakeholders
C. Reviewing the business strategy
D. Conducting a business impact analysis (BIA)

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 430
The **MAIN** purpose of documenting information security guidelines for use within a large, international organization is to:

A. ensure that all business units have the same strategic security goals.
B. provide evidence for auditors that security practices are adequate.
C. explain the organization's preferred practices for security.
D. ensure that all business units implement identical security procedures.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
QUESTION 431
Which of the following should be an information security manager's **PRIMARY** role when an organization initiates a data classification process?

A. Verify that assets have been appropriately classified.
B. Apply security in accordance with specific classification.
C. Define the classification structure to be implemented.
D. Assign the asset classification level.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 432
Which of the following should be an information security manager's **FIRST** course of action following a decision to implement a new technology?

A. Determine security controls needed to support the new technology.
B. Perform a business impact analysis (BIA) on the new technology.
C. Perform a return-on-investment (ROI) analysis for the new technology.
D. Determine whether the new technology will comply with regulatory requirements.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 433
Which of the following defines the minimum security requirements that a specific system must meet?

A. Security policy
B. Security guideline
C. Security procedure
D. Security baseline
Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 434
An organization recently rolled out a new procurement program that does not include any security requirements. Which of the following should the information security manager do **FIRST**?

A. Conduct security assessments of vendors based on value of annual spend with each vendor.
B. Meet with the head of procurement to discuss aligning security with the organization's operational objectives.
C. Ask internal audit to conduct an assessment of the current state of third-party security controls.
D. Escalate the procurement program gaps to the compliance department in case of noncompliance issues.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 435
Which of the following would be **MOST** helpful in gaining support for a business case for an information security initiative?

A. Demonstrating organizational alignment
B. Emphasizing threats to the organization
C. Referencing control deficiencies
D. Presenting a solution comparison matrix

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 436
When drafting the corporate privacy statement for a public web site, which of the following **MUST** be included?

A. Access control requirements
B. Limited liability clause
C. Information encryption requirements
D. Explanation of information usage

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 437
Which of the following is **BEST** to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?

A. Estimated reduction in risk
B. Estimated increase in efficiency
C. Projected costs over time
D. Projected increase in maturity level

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 438

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

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 439
In an organization, information systems security is the responsibility of:

A. all personnel.
B. information systems personnel.
C. information systems security personnel.
D. functional personnel.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 440
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 441
The MAIN goal of an information security strategic plan is to:

A. develop a risk assessment plan.
B. develop a data protection plan.
C. protect information assets and resources.
D. establish security governance.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 442
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 443
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 444
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
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 445
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: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 446
Which of the following will **BEST** facilitate the development of appropriate incident response procedures?

A. Conducting scenario testing
B. Performing vulnerability assessments

C. Analyzing key risk indicators (KRIs)
D. Assessing capability maturity

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 447
An organization is considering a self-service solution for the deployment of virtualized development servers. Which of the following should be the information security manager's **PRIMARY** concern?

A. Ability to maintain server security baseline
B. Ability to remain current with patches
C. Generation of excessive security event logs
D. Segregation of servers from the production environment

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 448
Which of the following activities would **BEST** incorporate security into the software development life cycle (SDLC)?

A. Minimize the use of open source software.
B. Include security training for the development team.
C. Scan operating systems for vulnerabilities.
D. Test applications before go-live.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 449
Which of the following should be the **MOST** important consideration when implementing an information security framework?

A. Compliance requirements
B. Audit findings
C. Risk appetite
D. Technical capabilities

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT
Explanation

Explanation/Reference:

QUESTION 450
A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:

A. contact the employees involved to retake security awareness training
B. notify senior management that employees are breaching policy
C. limit access to the Internet for employees involved
D. initiate an investigation to determine the full extent of noncompliance

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 451
To address the issue that performance pressures on IT may conflict with information security controls, it is **MOST** important that:

A. noncompliance issues are reported to senior management
B. information security management understands business performance issues
C. the security policy is changed to accommodate IT performance pressure
D. senior management provides guidance and dispute resolution

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 452
Which of the following would be **MOST** effective in the strategic alignment of security initiatives?

A. A security steering committee is set up within the IT department.

B. Key information security policies are updated on a regular basis.
C. Business leaders participate in information security decision making.
D. Policies are created with input from business unit managers.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 453
Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Ensure that proper controls exist for code review and release management
B. Set up an agent to run a virus-scanning program across platforms
C. Implement controls for continuous monitoring of middleware transactions
D. Apply the latest patch programs to the production operating systems

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 454
The BEST way to mitigate the risk associated with a social engineering attack is to:

A. deploy an effective intrusion detection system (IDS)
B. perform a user-knowledge gap assessment of information security practices
C. perform a business risk assessment of the email filtering system
D. implement multi-factor authentication on critical business systems

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 455
When considering whether to adopt a new information security framework, an organization's information security manager should FIRST:

A. compare the framework with the current business strategy
B. perform a technical feasibility analysis
C. perform a financial viability study
D. analyze the framework's legal implications and business impact

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 456
After detecting an advanced persistent threat (APT), which of the following should be the information security manager's FIRST step?

A. Notify management
B. Contain the threat
C. Remove the threat
D. Perform root-cause analysis

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 457
A new system has been developed that does not comply with password-aging rules. This noncompliance can BEST be identified through:

A. a business impact analysis
B. an internal audit assessment
C. an incident management process
D. a progressive series of warnings

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 458
Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

A. Client logins are subject to replay attack
B. Compromised VPN clients could impact the network
C. Attackers could compromise the VPN gateway
D. VPN traffic could be sniffed and captured

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Reference: https://resources.infosecinstitute.com/importance-effective-vpn-remote-access-policy/#gref

QUESTION 459
In which of the following ways can an information security manager BEST ensure that security controls are adequate for supporting business goals and objectives?

A. Reviewing results of the annual company external audit
B. Adopting internationally accepted controls
C. Enforcing strict disciplinary procedures in case of noncompliance
D. Using the risk management process

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 460
The authorization to transfer the handling of an internal security incident to a third-party support provider is PRIMARILY defined by the:

A. information security manager
B. escalation procedures
C. disaster recovery plan
D. chain of custody

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 461
Which of the following outsourced services has the GREATEST need for security monitoring?

A. Enterprise infrastructure
B. Application development
C. Virtual private network (VPN) services
D. Web site hosting

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 462
Which of the following is done PRIMARILY to address the integrity of information?

A. Assignment of appropriate control permissions
B. Implementation of an Internet security application
C. Implementation of a duplex server system
D. Encryption of email

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 463
A multinational organization's information security manager has been advised that the city in which a contracted regional data center is located is experiencing civil unrest. The information security manager should FIRST:

A. delete the organization's sensitive data at the provider's location
B. engage another service provider at a safer location
C. verify the provider's ability to protect the organization's data
D. evaluate options to recover if the data center becomes unreachable

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 464
When defining responsibilities with a cloud computing vendor, which of the following should be regarded as a shared responsibility between user and provider?

A. Data ownership
B. Access log review
C. Application logging
D. Incident response

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 465
An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:
A. map the strategy to business objectives
B. perform a cost-benefit analysis
C. conduct a risk assessment
D. develop a business case

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 466
An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

A. Requiring the backup of the organization's data by the user
B. Establishing the authority to remote wipe
C. Monitoring how often the smartphone is used
D. Developing security awareness training

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 467

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

A. Eradication
B. Review
C. Containment
D. Identification

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 468
Employees in a large multinational organization frequently travel among various geographic locations. Which type of authorization policy **BEST** addresses this practice?

A. Multilevel
B. Identity
C. Role-based
D. Discretionary

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 469
To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:

A. assess security during equipment deployment.
B. ensure compliance during user acceptance testing.
C. assess the risks of all new equipment.
D. develop an approved equipment list.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 470
Segregation of duties is a security control **PRIMARILY** used to:

A. establish dual check.

B. establish hierarchy.
C. limit malicious behavior.
D. decentralize operations.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 471
Which of the following is the **BEST** approach when using sensitive customer data during the testing phase of a systems development project?

A. Establish the test environment on a separate network.
B. Sanitize customer data.
C. Monitor the test environment for data loss.
D. Implement equivalent controls to those on the source system.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 472

Which of the following analyses will **BEST** identify the external influences to an organization's information security?

A. Gap analysis
B. Business impact analysis
C. Threat analysis
D. Vulnerability analysis.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 473
Spoofing should be prevented because it may be used to:

A. assemble information, track traffic, and identify network vulnerabilities.
B. predict which way a program will branch when an option is presented.
C. gain illegal entry to a secure system by faking the sender's address.
D. capture information such as password traveling through the network.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 474
Utilizing external resources for highly technical information security tasks allows an information security manager to:

A. distribute technology risk.
B. leverage limited resources.
C. outsource responsibility.
D. transfer business risk.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 475
An information security team is investigating an alleged breach of an organization's network. Which of the following would be the **BEST** single source of evidence to review?

A. Intrusion detection system
B. SIEM tool
C. Antivirus software
D. File integrity monitoring software

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 476
After logging in to a web application, further password credentials are required at various application points. Which of the following is the **PRIMARY** reason for such an approach?

A. To ensure access is granted to the authorized person
B. To enforce strong two-factor authentication
C. To ensure session management variables are secure
D. To implement single sign-on

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 477
The **MAIN** reason for continuous monitoring of a security strategy is to:

A. optimize resource allocation.

B. confirm benefits are being realized.
C. evaluate the implementation of the strategy.
D. allocate funds for information security

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 478
Which of the following is the **MOST** important factor in an organization's selection of a key risk indicator (KRI)?

A. Return on investment
B. Organizational culture
C. Compliance requirements
D. Criticality of information

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 479
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

A. baseline security controls.
B. cost-benefit analyses.
C. benchmarking security metrics.
D. security objectives.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 480
In an organization that has undergone an expansion through an acquisition which of the following would **BEST** secure the enterprise network?

A. Using security groups
B. Log analysis of system access
C. Business or role-based segmentation
D. Encryption of data traversing networks

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 481
An organization has established information security policies, but the information security manager has noted a large number of exception requests. Which of the following is the **MOST** likely reason for this situation?

A. The organization is operating in a highly regulated industry.
B. The information security program is not adequately funded.
C. The information security policies lack alignment with corporate goals.
D. The information security policies are not communicated across the organization

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 482
An organization shares customer information across its globally dispersed branches. Which of the following should be the **GREATEST** concern to information security management?

A. Cross-cultural differences between branches
B. Conflicting data protection regulations
C. Insecure wide area networks (WANs)

D. Decentralization of information security

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 483
Which of the following provides the **MOST** comprehensive understanding of an organization's information security posture?
A. Risk management metrics
B. External audit findings
C. Results of vulnerability assessments
D. The organization's security incident trends

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 484
Most security vulnerabilities in software exit because:

A. security features are not tested adequately.
B. software has undocumented features.
C. security is not properly designed.
D. software is developed without adherence to standards.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 485

Which of the following is a potential indicator of inappropriate Internet use by staff?

A. Increased help desk calls for password resets
B. Reduced number of pings on firewalls
C. Increased reports of slow system performance
D. Increased number of weakness from vulnerability scans

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 486
A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The **GREATEST** weakness under this system architecture is that:

A. users can gain direct access to the application ID and circumvent data controls.
B. when multiple sessions with the same application ID collide, the database locks up.
C. the database becomes unavailable if the password of the application ID expires.
D. an incident involving unauthorized access to data cannot be tied to a specific user.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 487
An organization has decided to implement a security information and event management (SIEM) system. It is **MOST** important for the organization to consider:

A. industry best practices.
B. data ownership.
C. log sources.
D. threat assessments.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 488
Which of the following change management procedures is **MOST** likely to cause concern to the information security manager?

A. Fallback processes are tested the weekend before changes are made.

B. The development manager migrates programs into production.
C. A manual rather than an automated process is used to compare program versions.
D. Users are not notified of scheduled system changes.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 489
Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed **NEXT**?

A. Develop an implementation strategy.
B. Schedule the target end date for implementation activities.
C. Budget the total cost of implementation activities.
D. Calculate the residual risk for each countermeasure.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 490
Which of the following would **BEST** assist an IS manager in gaining strategic support from executive management?

A. Annual report of security incidents within the organization
B. Research on trends in global information security breaches
C. Rating of the organization's security, based on international standards
D. Risk analysis specific to the organization

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 491
An emergency change was made to an IT system as a result of a failure. Which of the following should be of **GREATEST** concern to the organization's information security manager?

A. The change did not include a proper assessment of risk.
B. Documentation of the change was made after implementation.
C. The information security manager did not review the change prior to implementation.
D. The operations team implemented the change without regression testing.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 492
Which of the following is the **MOST** important reason for performing vulnerability assessments periodically?

A. Management requires regular reports.
B. The environment changes constantly.
C. Technology risks must be mitigated.
D. The current threat levels are being assessed.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 493
A business case for investment in an information security management infrastructure **MUST** include:

A. evidence that the proposed infrastructure is certified.
B. specifics on the security applications needed.
C. data management methods currently in use.
D. impact of noncompliance with applicable standards.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 494
Which of the following threats is prevented by using token-based authentication?

A. Password sniffing attack on the network
B. Denial of service attack over the network
C. Main-in-the middle attack on the client
D. Session eavesdropping attack on the network

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 495
Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

A. Data ownership
B. Data monitoring
C. Data custodian

D. Data encryption

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 496
When outsourcing data to a cloud service provider, which of the following should be the information security manager's **MOST** important consideration?

A. Roles and responsibilities have been defined for the subscriber organization.
B. Cloud servers are located in the same country as the organization.
C. Access authorization includes biometric security verification.
D. Data stored at the cloud service provider is not co-mingled.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 497
Without prior approval, a training department enrolled the company in a free cloud-based collaboration site and invited employees to use it. Which of the following is the **BEST** response of the information security manager?

A. Conduct a risk assessment and develop an impact analysis.
B. Update the risk register and review the information security strategy.
C. Report the activity to senior management.
D. Allow temporary use of the site and monitor for data leakage.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 498
Which of the following is **MOST** likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

A. The activities being monitored deviate from what is considered normal.
B. The information regarding monitored activities becomes stale.
C. The pattern of normal behavior changes quickly and dramatically.
D. The environment is complex.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 499
Which of the following will **BEST** protect confidential data when connecting large wireless networks to an existing wired-network infrastructure?

A. Mandatory access control (MAC) address filtering
B. Strong passwords
C. Virtual private network (VPN)
D. Firewall

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 500
A global organization processes and stores large volumes of personal data. Which of the following would be the MOST important attribute in creating a data access policy?

A. Availability
B. Integrity
C. Reliability
D. Confidentiality

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 501
Which of the following is MOST important for an information security manager to regularly report to senior management?
A. Results of penetration tests
B. Audit reports
C. Impact of unremediated risks
D. Threat analysis reports

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 502
Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

A. Automation of controls
B. Documentation of control procedures
C. Integration of assurance efforts
D. Standardization of compliance requirements

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 503
Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

A. Warm
B. Redundant
C. Shared
D. Mobile

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:
Reference: https://searchdisasterrecovery.techtarget.com/answer/Whats-the-difference-between-a-hot-site-and-cold-site-for-disaster-recovery

QUESTION 504
Which of the following characteristics is MOST important to a bank in a high-value online financial transaction system?

A. Identification
B. Confidentiality
C. Authentication
D. Audit monitoring

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 505
Which of the following would MOST likely require a business continuity plan to be invoked?

A. An unauthorized visitor discovered in the data center
B. A distributed denial of service attack on an e-mail server
C. An epidemic preventing staff from performing job functions
D. A hacker holding personally identifiable information hostage

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 506
An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

A. Business impact if threats materialize
B. Availability of unused funds in the security budget
C. Threat information from reputable sources
D. Alignment of the new initiative with the approved business strategy

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 507
When messages are encrypted and digitally signed to protect documents transferred between trading partners, the **GREATEST** concern is that:

A. trading partners can repudiate the transmission of messages.
B. hackers can eavesdrop on messages.
C. trading partners can repudiate the receipt of messages.
D. hackers can introduce forgery messages.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 508
Of the following, who should have **PRIMARY** responsibility for assessing the security risk associated with an outsourced cloud provider contract?

A. Information security manager
B. Compliance manager

C. Chief information officer
D. Service delivery manager

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 509
Which of the following would **BEST** provide stakeholders with information to determine the appropriate response to a disaster?

A. Risk assessment
B. Vulnerability assessment
C. Business impact analysis
D. SWOT analysis

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 510
The **PRIMARY** purpose for continuous monitoring of security controls is to ensure:

A. system availability.
B. control gaps are minimized.
C. effectiveness of controls.
D. alignment with compliance requirements.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 511
To prevent computers on the corporate network from being used as part of a distributed denial of service attack, the information security manager should use:

A. incoming traffic filtering
B. outgoing traffic filtering
C. IT security policy dissemination
D. rate limiting
Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 512
Which of the following is the **PRIMARY** objective of reporting security metrics to stakeholders?

A. To identify key controls within the organization
B. To provide support for security audit activities
C. To communicate the effectiveness of the security program
D. To demonstrate alignment to the business strategy

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 513
Which of the following **BEST** reduces the likelihood of leakage of private information via email?

A. Email encryption
B. User awareness training
C. Strong user authentication protocols
D. Prohibition on the personal use of email

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 514
Once a suite of security controls has been successfully implemented for an organization's business units, it is **MOST** important for the information security manager to:
A. ensure the controls are regularly tested for ongoing effectiveness.
B. hand over the controls to the relevant business owners.
C. prepare to adapt the controls for future system upgrades.
D. perform testing to compare control performance against industry levels.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 515
What should be an organization's **MAIN** concern when evaluating an Infrastructure as a Service (IaaS) cloud computing model for an e-commerce application?

A. Availability of provider's services
B. Internal audit requirements
C. Where the application resides
D. Application ownership

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 516
Which of the following would be **MOST** important to include in a bring your own device (BYOD) policy with regard to lost or stolen devices? The need for employees to:

A. initiate the company's incident reporting process.
B. seek advice from the mobile service provider.
C. notify local law enforcement.
D. request a remote wipe of the device.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 517
An information security manager learns that the root password of an external FTP server may be subject to brute force attacks. Which of the following would be the **MOST** appropriate way to reduce the likelihood of a successful attack?

A. Block the source IP address of the attacker.
B. Lock remote logon after multiple failed attempts.
C. Disable access to the externally facing server.
D. Install an intrusion detection system (IDS).

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 518
An advantage of antivirus software schemes based on change detection is that they have:

A. a chance of detecting current and future viral strains.
B. a more flexible directory of viral signatures.
C. to be updated less frequently than activity monitors.
D. the highest probability of avoiding false alarms.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 519
Which of the following is the **BEST** performed by the security department?

A. Approving standards for accessing the operating system
B. Logging unauthorized access to the operating system
C. Managing user profiles for accessing the operating system
D. Provisioning users to access the operating system

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 520
An organization outsources its payroll processing. Which of the following would be the **BEST** key risk indicator for monitoring the information security of the service provider?

A. Number of security incidents by severity
B. Number of critical security patches
C. Percentage of application up-time
D. Number of manual payroll adjustments

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 521
Ensuring that activities performed by outsourcing providers comply with information security policies can **BEST** be accomplished through the use of:

A. service level agreements.
B. independent audits.
C. explicit contract language.
D. local regulations.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 522
Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered the **MOST** significant exposure?

A. Proxy server
B. Mail relay server
C. Application server
D. Database server

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 523
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities **BEST** supports the concept of integrity?

A. Enforcing service level agreements
B. Implementing a data classification schema
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 524
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the **GREATEST** concern to an information security manager if omitted from the contract?

A. Authority of the subscriber to approve access to its data
B. Right of the subscriber to conduct onsite audits of the vendor
C. Escrow of software code with conditions for code release
D. Comingling of subscribers' data on the same physical server

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 525
Which of the following is the **BEST** method to protect consumer private information for an online public website?

A. Encrypt consumer's data in transit and at rest.
B. Apply a masking policy to the consumer data.
C. Use secure encrypted transport layer.
D. Apply strong authentication to online accounts.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 526
For an organization with a large and complex IT infrastructure, which of the following elements of a disaster recovery hot site service will require the closest monitoring?

A. Employee access

B. Audit rights
C. Systems configurations
D. Number of subscribers

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 527
Which of the following metrics is the **BEST** indicator of an abuse of the change management process that could compromise information security?

A. Small number of change request
B. Large percentage decrease in monthly change requests
C. Percentage of changes that include post-approval supplemental add-ons
D. High ratio of lines of code changed to total lines of code

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 528
Which of the following is the **MOST** effective data loss control when connecting a personally owned mobile device to the corporate email system?

A. Email must be stored in an encrypted format on the mobile device.
B. Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
C. A senior manager must approve each connection.
D. Users must agree to allow the mobile device to be wiped if it is lost.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 529
The use of a business case to obtain funding for an information security investment is **MOST** effective when the business case:

A. relates information security policies and standards into business requirements
B. relates the investment to the organization's strategic plan.
C. realigns information security objectives to organizational strategy.
D. articulates management's intent and information security directives in clear language.
Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 530
The PRIMARY reason for defining the information security roles and responsibilities of staff throughout an organization is to:

A. reinforce the need for training
B. increase corporate accountability
C. comply with security policy
D. enforce individual accountability

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 531
A validated patch to address a new vulnerability that may affect a mission-critical server has been released.

What should be done immediately?

A. Add mitigating controls.
B. Check the server's security and install the patch.
C. Conduct an impact analysis.
D. Take the server off-line and install the patch.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 532
Which of the following is the **MOST** effective way to protect the authenticity of data in transit?

A. Hash value
B. Digital signature
C. Public key
D. Private key

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 533
Which of the following is the **FIRST** task when determining an organization's information security profile?

A. Build an asset inventory
B. List administrative privileges
C. Establish security standards
D. Complete a threat assessment

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 534
What would be the P**RIMARY** reason for an organization to conduct a simulated phishing attack on its employees as part of a social engineering assessment?

A. Measure the effectiveness of security awareness training.

B. Identify the need for mitigating security controls.
C. Measure the effectiveness of the anti-spam solution.
D. Test the effectiveness of the incident response plan.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 535
Which of the following activities should take place **FIRST** when a security patch for Internet software is received from a vendor?

A. The patch should be validated using a hash algorithm.
B. The patch should be applied to critical systems.
C. The patch should be deployed quickly to systems that are vulnerable.
D. The patch should be evaluated in a testing environment.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 536
Which of the following would **BEST** ensure that application security standards are in place?

A. Functional testing
B. Performing a code review
C. Publishing software coding standards
D. Penetration testing

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 537
Which of the following is the **BEST** criterion to use when classifying assets?

A. The market value of the assets
B. Annual loss expectancy (ALE)
C. Value of the assets relative to the organization
D. Recovery time objective (RTO)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 538
Which of the following is the MOST effective method to prevent a SQL injection in an employee portal?

A. Reconfigure the database schema
B. Enforce referential integrity on the database
C. Conduct code reviews
D. Conduct network penetration testing

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 539
Which of the following is **MOST** important when conducting a forensic investigation?

A. Documenting analysis steps
B. Capturing full system images

C. Maintaining a chain of custody
D. Analyzing system memory

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 540
Which of the following is the **BEST** indication of information security strategy alignment with the business?

A. Number of business objectives directly supported by information security initiatives.
B. Percentage of corporate budget allocated to information security initiatives.
C. Number of business executives who have attended information security awareness sessions.
D. Percentage of information security incidents resolved within defined service level agreements.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 541
When customer data has been compromised, an organization should contact law enforcement authorities:

A. if the attack comes from an international source.
B. when directed by the information security manager.
C. if there is potential impact to the organization.
D. in accordance with the corporate communication policy.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 542
The **GREATEST** benefit of choosing a private cloud over a public cloud would be:

A. server protection.
B. collection of data forensics.
C. online service availability.
D. containment of customer data.
Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 543
Organization A offers e-commerce services and uses secure transport protocol to protect Internet communication. To confirm communication with Organization A, which of the following would be the **BEST** for a client to verify?

A. The certificate of the e-commerce server
B. The browser's indication of SSL use
C. The IP address of the e-commerce server
D. The URL of the e-commerce server

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 544
An information security steering group should:

A. provide general oversight and guidance.
B. develop information security policies.
C. establish information security baselines.
D. oversee the daily operations of the security program.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 545
Which of the following is an example of a vulnerability?

A. Natural disasters
B. Defective software
C. Ransomware
D. Unauthorized users

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 546
What would be an information security manager's **BEST** recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization's critical data?

A. Create an addendum to the existing contract.
B. Cancel the outsourcing contract.
C. Transfer the risk to the provider.
D. Initiate an external audit of the provider's data center.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 547

Which of the following is **MOST** important to include in monthly information security reports to the broad?

A. Trend analysis of security metrics
B. Threat intelligence
C. Root cause analysis of security incidents
D. Risk assessment results

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 548
Which of the following could be detected by a network intrusion detection system (IDS)?

A. Undocumented open ports
B. Unauthorized file change
C. Internally generated attacks
D. Emailed virus attachments

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 549
Which of the following is **MOST** important for an information security manager to verify before conducting full-functional continuity testing?

A. Risk acceptance by the business has been documented.
B. Incident response and recovery plans are documented in simple language.
C. Teams and individuals responsible for recovery have been identified.
D. Copies of recovery and incident response plans are kept offsite.

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 550
Which of the following would **BEST** detect malicious damage arising from an internal threat?

A. Access control list
B. Encryption
C. Fraud awareness training
D. Job rotation

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 551
Which of the following is **MOST** important for an information security manager to communicate to senior management regarding the security program?

A. Potential risks and exposures
B. Impact analysis results
C. Security architecture changes
D. User roles and responsibilities

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 552
Which of the following is the **BEST** defense against a brute force attack?

A. Discretionary access control
B. Intruder detection lockout
C. Time-of-day restrictions
D. Mandatory access control

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 553
An organization determines that an end-user has clicked on a malicious link. Which of the following would **MOST** effectively prevent similar situations from recurring?

A. End-user training
B. Virus protection
C. End-user access control
D. Updated security policies

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 554
An organization with a large number of users finds it necessary to improve access control applications. Which of the following would **BEST** help to prevent unauthorized user access to networks and applications?

A. Single sign-on
B. Biometric systems
C. Complex user passwords
D. Access control lists

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 555
Senior management has endorsed a comprehensive information security policy. Which of the following should the organization do **NEXT**?

A. Promote awareness of the policy among employees.
B. Seek policy buy-in from business stakeholders.
C. Implement an authentication and authorization system.
D. Identify relevant information security frameworks for adoption.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 556
The **PRIMARY** disadvantage of using a cold-site recovery facility is that it is:

A. unavailable for testing during normal business hours.
B. only available if not being used by the primary tenant.
C. not possible to reserve test dates in advance.
D. not cost-effective for testing critical applications at the site.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 557
Which of the following is the **BEST** way to demonstrate to senior management that organizational security practices comply with industry standards?

A. Results of an independent assessment
B. Up-to-date policy and procedures documentation
C. A report on the maturity of controls

D. Existence of an industry-accepted framework

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 558
The **BEST** way to report to the board on the effectiveness of the information security program is to present:

A. a dashboard illustrating key performance metrics.
B. peer-group industry benchmarks.
C. a summary of the most recent audit findings.
D. a report of cost savings from process improvements.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 559
Senior management has expressed concern that the organization's intrusion prevention system may repeatedly disrupt business operations. Which of the following **BEST** indicates that the information security manager has tuned the system to address this concern?

A. Decreasing false positives
B. Decreasing false negatives
C. Increasing false positives
D. Increasing false negatives

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 560

A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?

A. Add mitigating controls.
B. Take the server off-line and install the patch.
C. Check the server's security and install the patch.
D. Conduct an impact analysis.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 561
Which of the following is **MOST** helpful to maintain cohesiveness within an organization's information security resource?

A. Information security architecture
B. Security gap analysis
C. Business impact analysis
D. Information security steering committee

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 562
During a review to approve a penetration test plan, which of the following should be an information security manager's **PRIMARY** concern?

A. Penetration test team's deviation from scope
B. Unauthorized access to administrative utilities
C. False positive alarms to operations staff
D. Impact on production systems

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 563
Which of the following is **MOST** relevant for an information security manager to communicate to IT operations?
A. The level of inherent risk
B. Vulnerability assessments
C. Threat assessments
D. The level of exposure

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 564
Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have his, her password reset?

A. Performing reviews of password resets
B. Conducting security awareness programs
C. Increasing the frequency of password changes
D. Implementing automatic password syntax checking

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Social engineering can be mitigated best through periodic security awareness training for staff members who may be the target of such an attempt. Changing the frequency of password changes, strengthening passwords and checking the number of password resets may be desirable, but they will not be as effective in reducing the likelihood of a social engineering attack.

QUESTION 565
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 do not reflect awareness levels, but may prompt further research to confirm.

QUESTION 566
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 567
Which of the following change management activities would be a clear indicator that normal operational procedures require examination? A high percentage of:

A. similar change requests.
B. change request postponements.
C. canceled change requests.
D. emergency change requests.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A high percentage of emergency change requests could be caused by changes that are being introduced at the last minute to bypass normal chance management procedures. Similar requests, postponements and canceled requests all are indicative of a properly functioning change management process.

QUESTION 568
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 569
When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

A. submit the issue to the steering committee.
B. conduct an impact analysis to quantify the risks.

C. isolate the system from the rest of the network.
D. request a risk acceptance from senior management.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:
Explanation:

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

QUESTION 570
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 571
Nonrepudiation can BEST be assured by using:

A. delivery path tracing.
B. reverse lookup translation.
C. out-of-hand channels.
D. digital signatures.

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 572
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 573
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 574
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 575
The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performance.
B. use a honeypot to check for unusual activity.
C. audit the configuration of the IDS.
D. benchmark the IDS against a peer site.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Simulating an attack on the network demonstrates whether the intrusion detection system (IDS) is properly tuned. Reviewing the configuration may or may not reveal weaknesses since an anomaly-based system uses trends to identify potential attacks. A honeypot is not a good first step since it would need to have already been penetrated. Benchmarking against a peer site would generally not be practical or useful.

QUESTION 576
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 577
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 578
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 579
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
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 580
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 581
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 582

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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 583
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 584
Which of the following represents a PRIMARY area of interest when conducting a penetration test?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 585
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 586
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 587
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 588
An information security manager suspects that the organization has suffered a ransomware attack. What should be done FIRST?

A. Notify senior management.
B. Alert employees to the attack.

C. Confirm the infection.
D. Isolate the affected systems.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 589
The **MAIN** reason for internal certification of web-based business applications is to ensure:
A. compliance with industry standards.
B. changes to the organizational policy framework are identified.
C. up-to-date web technology is being used.
D. compliance with organizational policies.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 590
Knowing which of the following is **MOST** important when the information security manager is seeking senior management commitment?

A. Security costs
B. Technical vulnerabilities
C. Security technology requirements
D. Implementation tasks

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 591
Which of the following is **MOST** critical for prioritizing actions in a business continuity plan (BCP)?

A. Business impact analysis (BIA)
B. Risk assessment
C. Asset classification
D. Business process mapping

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 592
The **PRIMARY** benefit of integrating information security risk into enterprise risk management is to:

A. ensure timely risk mitigation.
B. justify the information security budget.
C. obtain senior management's commitment.
D. provide a holistic view of risk.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 593
After an information security business case has been approved by senior management, it should be:

A. used to design functional requirements for the solution.
B. used as the foundation for a risk assessment.
C. referenced to build architectural blueprints for the solution.
D. reviewed at key intervals to ensure intended outcomes.

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 594
The **BEST** way to isolate corporate data stored on employee-owned mobile devices would be to implement:

A. a sandbox environment.
B. device encryption.
C. two-factor authentication.
D. a strong password policy.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 595
For a user of commercial software downloaded from the Internet, which of the following is the **MOST** effective means of ensuring authenticity?

A. Digital signatures
B. Digital certificates
C. Digital code signing
D. Steganography

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 596
Due to budget constraints, an internal IT application does not include the necessary controls to meet a client service level agreement (SLA).

Which of the following is the information security manager's **BEST** course of action?

A. Inform the legal department of the deficiency.
B. Analyze and report the issue to senior management.
C. Require the application owner to implement the controls.
D. Assess and present the risks to the application owner.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 597
Which of the following is the **GREATEST** benefit of integrating a security information and event management (SIEM) solution with traditional security tools such as IDS, anti-malware, and email screening solutions?

A. The elimination of false positive detections
B. A reduction in operational costs
C. An increase in visibility into patterns of potential threats
D. The consolidation of tools into a single console

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 598
An organization is **MOST** at risk from a new worm being introduced through the intranet when:

A. desktop virus definition files are not up to date.
B. system software does not undergo integrity checks.
C. hosts have static IP addresses.
D. executable code is run from inside the firewall.

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 599
A risk analysis for a new system is being performed.

For which of the following is business knowledge **MORE** important than IT knowledge?
A. Vulnerability analysis
B. Balanced scorecard
C. Cost-benefit analysis
D. Impact analysis

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 600
Which of the following is **MOST** likely to drive an update to the information security strategy?

A. A recent penetration test has uncovered a control weakness.
B. A major business application has been upgraded.
C. Management has decided to implement an emerging technology.
D. A new chief technology officer has been hired.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 601
A risk has been formally accepted and documented.

Which of the following is the **MOST** important action for an information security manager?

A. Update risk tolerance levels.
B. Notify senior management and the board.
C. Monitor the environment for changes.
D. Re-evaluate the organization's risk appetite.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 602
From a business perspective, the **MOST** important function of information security is to support:

A. predictable operations.
B. international standards.
C. security awareness.
D. corporate policy.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 603
Which of the following is the **MOST** effective method for assessing the effectiveness of a security awareness program?

A. Post-incident review
B. Social engineering test
C. Vulnerability scan
D. Tabletop test

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 604
In a resource-restricted security program, which of the following approaches will provide the **BEST** use of the limited resources?

A. Cross-training
B. Risk avoidance
C. Risk prioritization
D. Threat management

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 605
An organization will be outsourcing mission-critical processes.

Which of the following is **MOST** important to verify before signing the service level agreement (SLA)?

A. The provider has implemented the latest technologies.
B. The provider's technical staff are evaluated annually.
C. The provider is widely known within the organization's industry.
D. The provider has been audited by a recognized audit firm.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 606

Which of the following should be the **PRIMARY** input when defining the desired state of security within an organization?

A. Acceptable risk level
B. Annual loss expectancy
C. External audit results
D. Level of business impact

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 607
The **MAIN** reason for an information security manager to monitor industry level changes in the business and IT is to:

A. evaluate the effect of the changes on the levels of residual risk.
B. identify changes in the risk environment.
C. update information security policies in accordance with the changes.
D. change business objectives based on potential impact.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 608
Exceptions to a security policy should be approved based **PRIMARILY** on:

A. risk appetite.
B. the external threat probability.
C. results of a business impact analysis (BIA).
D. the number of security incidents.

Correct Answer: C

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 609
Which of the following is the **BEST** way to increase the visibility of information security within an organization's culture?

A. Requiring cross-functional information security training
B. Implementing user awareness campaigns for the entire company
C. Publishing an acceptable use policy
D. Establishing security policies based on industry standards

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 610
Recovery time objectives (RTOs) are an output of which of the following?

A. Business continuity plan
B. Disaster recovery plan
C. Service level agreement (SLA)
D. Business impact analysis (BIA)

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 611
An organization's information security strategy for the coming year emphasizes reducing the risk of ransomware.

Which of the following would be **MOST** helpful to support this strategy?

A. Provide relevant training to all staff.
B. Create a penetration testing plan.
C. Perform a controls gap analysis.
D. Strengthen security controls for the IT environment.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 612
What would be an information security manager's **BEST** course of action when notified that the implementation of some security controls is being delayed due to budget constraints?

A. Prioritize security controls based on risk.
B. Request a budget exception for the security controls.
C. Begin the risk acceptance process.
D. Suggest less expensive alternative security controls.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 613
Relying on which of the following methods when detecting new threats using IDS should be of **MOST** concern?

A. Statistical pattern recognition
B. Attack signatures
C. Heuristic analysis
D. Traffic analysis

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 614
An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective.

Which of the following would **BEST** help the information security manager determine the security requirements to resolve the control deficiency?
A. Risk assessment
B. Gap analysis
C. Cost-benefit analysis
D. Business case

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 615
Which of the following is the **MOST** important step when establishing guidelines for the use of social networking sites in an organization?

A. Establish disciplinary actions for noncompliance.
B. Define acceptable information for posting.
C. Identity secure social networking sites.
D. Perform a vulnerability assessment.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 616

Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?

A. Key risk indicators (KRIs)
B. Capability maturity models
C. Critical success factors (CSFs)
D. Key performance indicators (KPIs)

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 617
Which of the following is the MOST important factor when determining the frequency of information security reassessment?

A. Risk priority
B. Risk metrics
C. Audit findings
D. Mitigating controls

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 618
Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?

A. Integrate industry best practices
B. Obtain senior management sign-off
C. Conduct an organization-wide security audit
D. Leverage security steering committee contribution

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 619
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Analyze vulnerabilities
B. Determine recovery priorities
C. Confirm control effectiveness
D. Define the recovery point objective (RPO)

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 620
An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?

A. Analyze findings from previous audit reports
B. Analyze results from training completion reports
C. Analyze results of a social engineering test
D. Analyze responses from an employee survey of training satisfaction

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 621
An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?

A. Perform regular audits on the implementation of critical patches.
B. Evaluate patch management training.
C. Assess the patch management process.
D. Monitor and notify IT staff of critical patches.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 622
A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

A. Invoke the right to audit per the contract
B. Review the provider's information security policy
C. Check references supplied by the provider's other customers
D. Review the provider's self-assessment

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 623
Which of the following is MOST important when selecting an information security metric?

A. Aligning the metric to the IT strategy
B. Defining the metric in quantitative terms
C. Ensuring the metric is repeatable
D. Defining the metric in qualitative terms

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 624
Which of the following BEST supports the risk assessment process to determine critically of an asset?

A. Business impact analysis (BIA)
B. Residual risk analysis
C. Vulnerability assessment
D. Threat assessment

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 625
When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

A. using https in place of http
B. coding standards and code review
C. consolidating multiple sites into a single portal
D. hardening of the web server's operating system

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 626
The PRIMARY benefit of integrating information security activities into change management processes is to:

A. ensure required controls are included in changes
B. protect the organization from unauthorized changes
C. provide greater accountability for security-related changes in the business

D. protect the business from collusion and compliance threats

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 627
Which of the following should be an information security manager's MOST important consideration when conducting a physical security review of a potential outsourced data center?

A. Distance of the data center from the corporate office
B. Availability of network circuit connections
C. Environment factors of the surrounding location
D. Proximity to law enforcement

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 628
Which of the following tools BEST demonstrates the effectiveness of the information security program?

A. Key risk indicators (KRIs)
B. Management satisfaction surveys
C. Risk heat map
D. A security balanced scorecard

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 629
In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:

A. segregation of duties policy
B. size of the IT security function
C. reporting line of the chief information security officer (CISO)
D. existence of an IT steering committee
Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 630
Which of the following would be an information security manager's PRIMARY challenge when deploying a Bring Your Own Device (BYOD) mobile program in an enterprise?

A. End user acceptance
B. Configuration management
C. Mobile application control
D. Disparate device security

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 631
When an operating system is being hardened, it is MOST important for an information security manager to ensure that:

A. system logs are activated
B. default passwords are changed
C. file access is restricted
D. anonymous access is removed

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 632
Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?
A. Requiring an external security audit of the IT service provider
B. Defining information security requirements with internal IT
C. Requiring regular reporting from the IT service provider
D. Defining the business recovery plan with the IT service provider

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 633
Which of the following would present the GREATEST need to revise information security policies?

A. A merger with a competing company
B. An increase in reported incidents
C. Implementation of a new firewall
D. Changes in standards and procedures

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 634
Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?

A. Number of published application-recovery plans
B. Ratio of recovery-plan documents to total applications
C. Ratio of tested applications to total applications
D. Ratio of successful to unsuccessful tests

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 635
During an annual security review of an organization's servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do FIRST?

A. Report the situation to the data owner
B. Remove access privileges to the folder containing the data
C. Isolate the server from the network
D. Train the customer service team on properly controlling file permissions

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 636
Which of the following is the BEST reason for delaying the application of a critical security patch?

A. Conflicts with software development lifecycle
B. Technology interdependencies
C. Lack of vulnerability management
D. Resource limitations

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 637
Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?

A. Internal audit reports
B. Application security policy
C. Vulnerability assessment results
D. A business case

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 638
Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?

A. Improved response time to incidents
B. Improved network protection
C. Enhanced forensic analysis
D. Reduced need for manual analysis

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 639
Which is MOST important when contracting an external party to perform a penetration test?

A. Provide network documentation
B. Obtain approval from IT management
C. Define the project scope

D. Increase the frequency of log reviews

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 640
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files
B. priority of restoration
C. point of synchronization
D. annual loss expectancy (ALE)

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 641
The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to communicate the:

A. status of the security posture
B. probability of future incidents
C. cost-benefit of security controls
D. risk acceptance criteria

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 642

An organization's HR department would like to outsource its employee system to a cloud-hosted solution due to features and cost savings offered. Management has identified this solution as a business need and wants to move forward. What should be the PRIMARY role of information security in this effort?

A. Explain security issues associated with the solution to management
B. Determine how to securely implement the solution
C. Ensure the service provider has the appropriate certifications
D. Ensure a security audit is performed of the service provider

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 643
Which of the following is MOST effective against system intrusions?

A. Two-factor authentication
B. Continuous monitoring
C. Layered protection
D. Penetration testing

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 644
The PRIMARY purpose of asset valuation for the management of information security is to:

A. prioritize risk management activities
B. eliminate the least significant assets
C. provide a basis for asset classification
D. determine the value of each asset

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 645
An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?

A. Report the risk and status of the information security program to the board
B. Revise the information security strategy to meet executive management's expectations
C. Escalate noncompliance concerns to the internal audit manager
D. Demonstrate alignment of the information security function with business needs

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 646
A recent audit has identified that security controls by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?

A. Discuss the issue with the data owners to determine the reason for the exception
B. Discuss the issue with data custodians to determine the reason for the exception
C. Report the issue to senior management and request funding to fix the issue
D. Deny access to the application until the issue is resolved

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 647

Which of the following is the PRIMARY role of a data custodian?

A. Validating information
B. Processing information
C. Classifying information
D. Securing information

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 648
Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection system.
B. Establish minimum security baselines.
C. Implement vendor recommended settings.
D. Perform periodic penetration testing.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 649
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 650
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 651
Which of the following are the MOST important individuals to include as members of an information security steering committee?

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

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 652
What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

A. Mandatory
B. Discretionary
C. Walled garden
D. Role-based

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Mandatory access controls restrict access to files based on the security classification of the file. This prevents users from sharing files with unauthorized users. Role-based access controls grant access according to the role assigned to a user; they do not prohibit file sharing. Discretionary and lattice-based access controls are not as effective as mandatory access controls in preventing file sharing. A walled garden is an environment that controls a user's access to web content and services. In effect, the walled garden directs the user's navigation within particular areas, and does not necessarily prevent sharing of other material.

QUESTION 653
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 654
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 655
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 656
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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
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 657
Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Reduced number of security violation reports
B. A quantitative evaluation to ensure user comprehension
C. Increased interest in focus groups on security issues
D. Increased number of security violation reports

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 658
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is critical to establish a clear understanding on what is permissible during the engagement. 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 659
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 660
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 661
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 662
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 663
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 664
Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

A. define the circumstances where cryptography should be used.
B. define cryptographic algorithms and key lengths.
C. describe handling procedures of cryptographic keys.
D. establish the use of cryptographic solutions.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

There should be documented standards-procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

QUESTION 665
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 666
What is the MOST appropriate change management procedure for the handling of emergency 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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 667
A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

A. Enable access through a separate device that requires adequate authentication
B. Implement manual procedures that require password change after each use
C. Request the vendor to add multiple user IDs
D. Analyze the logs to detect unauthorized access

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual. Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but. because it is detective, it would not be the most effective in this instance.

QUESTION 668
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 669
In business-critical applications, user access should be approved by the:

A. information security manager.
B. data owner.
C. data custodian.
D. business management.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

A data owner is in the best position to validate access rights to users due to their deep understanding of business requirements and of functional implementation within the application. This responsibility should be enforced by the policy. An information security manager will coordinate and execute the implementation of the

role-based access control. A data custodian will ensure that proper safeguards are in place to protect the data from unauthorized access; it is not the data custodian's responsibility to assign access rights. Business management is not. in all cases, the owner of the data.

QUESTION 670
In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 671
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 672
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

A. Review the procedures for granting access
B. Establish procedures for granting emergency access
C. Meet with data owners to understand business needs
D. Redefine and implement proper access rights

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

An information security manager must understand the business needs that motivated the change prior to taking any unilateral action. Following this, all other choices could be correct depending on the priorities set by the business unit.

QUESTION 673
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 674
Which of the following should be in place before a black box penetration test begins?

A. IT management approval
B. Proper communication and awareness training
C. A clearly stated definition of scope
D. An incident response plan

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Having a clearly stated definition of scope is most important to ensure a proper understanding of risk as well as success criteria, IT management approval may not be required based on senior management decisions. Communication, awareness and an incident response plan are not a necessary requirement. In fact, a penetration test could help promote the creation and execution of the incident response plan.

QUESTION 675
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 676

Which of the following events generally has the highest information security impact?

A. Opening a new office
B. Merging with another organization
C. Relocating the data center
D. Rewiring the network

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Merging with or acquiring another organization causes a major impact on an information security management function because new vulnerabilities and risks are inherited. Opening a new office, moving the data center to a new site, or rewiring a network may have information security risks, but generally comply with corporate security policy and are easier to secure.

QUESTION 677
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 678
An information security program should focus on:

A. best practices also in place at peer companies.

B. solutions codified in international standards.
C. key controls identified in risk assessments.
D. continued process improvement.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

Risk assessment identifies the appropriate controls to mitigate identified business risks that the program should implement to protect the business. Peer industry best practices, international standards and continued process improvement can be used to support the program, but these cannot be blindly implemented without the consideration of business risk.

QUESTION 679
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 680
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 681
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 682
To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

A. create a separate account for the programmer as a power user.
B. log all of the programmers' activity for review by supervisor.
C. have the programmer sign a letter accepting full responsibility.
D. perform regular audits of the application.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers' actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

QUESTION 683
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 684
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 685
The MOST important reason for formally documenting security procedures is to ensure:

A. processes are repeatable and sustainable.
B. alignment with business objectives.
C. auditability by regulatory agencies.
D. objective criteria for the application of metrics.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 686
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 687
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

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

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 688
Which would be the BEST recommendation to protect against phishing attacks?

A. Install an antispam system
B. Publish security guidance for customers

C. Provide security awareness to the organization's staff
D. Install an application-level firewall

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
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 689
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 690
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 691
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. guidelineD. baseline.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
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 692
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 693
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 primary reason to involve security in the systems development life cycle (SDLC).

QUESTION 694
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 695
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 696
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 training. Users would not have the knowledge to accurately interpret and report violations without user education and training.

QUESTION 697
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 698
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 699
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: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 700
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 701
An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
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 702
Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 703
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 704
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 705
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 706
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 outsourced. This protects both organizations. All other steps are contributory to the contractual agreement, but are not key.

QUESTION 707
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 708
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 709
The **MOST** important reason for an information security manager to be involved in the change management process is to ensure that:

A. security controls are updated regularly.
B. potential vulnerabilities are identified.
C. risks have been evaluated.
D. security controls drive technology changes.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 710
An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. The data owner
B. Internal IT audit
C. The data custodian
D. The information security manager
Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 711

Which of the following presents the **GREATEST** information security concern when deploying an identity and access management solution?

A. Complying with the human resource policy
B. Supporting multiple user repositories
C. Supporting legacy applications
D. Gaining end user acceptance

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 712
Which of the following is the **MOST** important outcome of testing incident response plans?

A. Staff is educated about current threats.
B. An action plan is available for senior management.
C. Areas requiring investment are identified.
D. Internal procedures are improved.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 713
Inadvertent disclosure of internal business information on social media is **BEST** minimized by which of the following?
A. Developing social media guidelines
B. Educating users on social media risks
C. Limiting access to social media sites
D. Implementing data loss prevention (DLP) solutions

Correct Answer: B

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 714
Which of the following metrics would provide management with the **MOST** useful information about the effectiveness of a security awareness program?

A. Increased number of downloads of the organization's security policy
B. Decreased number of security incidents
C. Increased number of reported security incidents
D. Decreased number of phishing attacks

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 715
Which of the following is the **MOST** important security consideration when using Infrastructure as a Service (IaaS)?

A. Backup and recovery strategy
B. Compliance with internal standards
C. User access management
D. Segmentation among tenants

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 716
Which of the following provides the **BEST** evidence that the information security program is aligned to the business strategy?

A. The information security program manages risk within the business's risk tolerance.

B. The information security team is able to provide key performance indicators (KPIs) to senior management.
C. Business senior management supports the information security policies.
D. Information security initiatives are directly correlated to business processes.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 717
Which of the following statements indicates that a previously failing security program is becoming successful?

A. The number of threats has been reduced.
B. More employees and stakeholders are attending security awareness programs.
C. The number of vulnerability false positives is decreasing.
D. Management's attention and budget are now focused on risk reduction.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 718
An external security audit has reported multiple instances of control noncompliance. Which of the following is **MOST** important for the information security manager to communicate to senior management?

A. Control owner responses based on a root cause analysis
B. The impact of noncompliance on the organization's risk profile
C. An accountability report to initiate remediation activities
D. A plan for mitigating the risk due to noncompliance

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 719
Which of the following is the **BEST** way for an organization that outsources many business processes to gain assurance that services provided are adequately secured?

A. Review the service providers' information security policies and procedures.
B. Conduct regular vulnerability assessments on the service providers' IT systems.
C. Perform regular audits on the service providers' applicable controls.
D. Provide information security awareness training to service provider staff.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 720
Which of the following will **BEST** facilitate the understanding of information security responsibilities by users across the organization?

A. Conducting security awareness training with performance incentives
B. Communicating security responsibilities as an acceptable usage policy
C. Warning users that disciplinary action will be taken for violations
D. Incorporating information security into the organization's code of conduct

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 721
Cold sites for disaster recovery events are **MOST** helpful in situations in which a company:

A. has a limited budget for coverage.
B. uses highly specialized equipment that must be custom manufactured.

C. is located in close proximity to the cold site.
D. does not require any telecommunications connectivity

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 722
An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's **FIRST** course of action?

A. Report the noncompliance to the board of directors.
B. Inform respective risk owners of the impact of exceptions
C. Design mitigating controls for the exceptions.
D. Prioritize the risk and implement treatment options.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 723
When multiple Internet intrusions on a server are detected, the **PRIMARY** concern of the information security manager should be to ensure that the:

A. server is backed up to the network.
B. server is unplugged from power.
C. integrity of evidence is preserved.
D. forensic investigation software is loaded on the server.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 724
An organization's information security manager has learned that similar organizations have become increasingly susceptible to spear phishing attacks. What is the BEST way to address this concern?

A. Update data loss prevention (DLP) rules for email.
B. Include tips to identify threats in awareness training.
C. Conduct a business impact analysis (BIA) of the threat.
D. Create a new security policy that staff must read and sign.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 725
The **BEST** defense against phishing attempts within an organization is:

A. filtering of e-mail.
B. an intrusion protection system (IPS).
C. strengthening of firewall rules.
D. an intrusion detection system (IDS).

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 726
Which of the following should be of **GREATEST** concern to a newly hired information security manager regarding security compliance?

A. Lack of risk assessments
B. Lack of standard operating procedures
C. Lack of security audits
D. Lack of executive support

Correct Answer: D

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 727
An organization wants to ensure its confidential data is isolated in a multi-tenanted environment at a well-known cloud service provider. Which of the following is the **BEST** way to ensure the data is adequately protected?

A. Obtain documentation of the encryption management practices.
B. Verify the provider follows a cloud service framework standard.
C. Ensure an audit of the provider is conducted to identify control gaps.
D. Review the provider's information security policies and procedures.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 728
When preparing a strategy for protection from SQL injection attacks, it is **MOST** important for the information security manager to involve:

A. senior management
B. the security operations center.
C. business owners.
D. application developers.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 729
Which of the following is the **MOST** challenging aspect of securing Internet of Things (IoT) devices?

A. Training staff on IoT architecture
B. Updating policies to include IoT devices
C. Managing the diversity of IoT architecture
D. Evaluating the reputations of IoT vendors

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 730
Which of the following is **MOST** likely to increase end user security awareness in an organization?

A. Simulated phishing attacks
B. Security objectives included in job descriptions
C. Red team penetration testing
D. A dedicated channel for reporting suspicious emails

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 731
Which of the following models provides a client organization with the **MOST** administrative control over a cloud-hosted environment?

A. Storage as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Software as a Service (SaaS)
D. Infrastructure as a Service (IaaS)

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 732
Which of the following is the **MAIN** concern when securing emerging technologies?

A. Applying the corporate hardening standards
B. Integrating with existing access controls
C. Unknown vulnerabilities
D. Compatibility with legacy systems

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 733
Which of the following is the **FIRST** step required to achieve effective performance measurement?

A. Select and place sensors
B. Implement control objectives
C. Validate and calibrate metrics
D. Define meaningful metrics

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 734
The **BEST** way to ensure information security efforts and initiatives continue to support corporate strategy is by:

A. including the CIO in the information security steering committee
B. conducting benchmarking with industry best practices

C. including information security metrics in the organizational metrics
D. performing periodic internal audits of the information security program

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 735
Which of the following is the **BEST** reason to separate short-term from long-term plans within an information security roadmap?

A. To allow for reactive initiatives
B. To update the roadmap according to current risks
C. To allocate resources for initiatives
D. To facilitate business plan reporting to management

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 736
An information security manager has been made aware that some employees are discussing confidential corporate business on social media sites.

Which of the following is the **BEST** response to this situation?
A. Communicate social media usage requirements and monitor compliance.
B. Block workplace access to social media sites and monitor employee usage.
C. Train employees how to set up privacy rules on social media sites.
D. Scan social media sites for company-related information.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 737
An organization is considering the purchase of a competitor. To determine the competitor's security posture, the **BEST** course of action for the organization's information security manager would be to:

A. assess the security policy of the competitor.
B. assess the key technical controls of the competitor.
C. conduct a penetration test of the competitor.
D. perform a security gap analysis on the competitor.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 738
A security team is conducting its annual disaster recovery test. Post-restoration testing shows the system response time is significantly slower due to insufficient bandwidth for Internet connectivity at the recovery center.

Which of the following is the security manager's **BEST** course of action?

A. Halt the test until the network bandwidth is increased.
B. Reduce the number of applications marked as critical.
C. Document the deficiency for review by business leadership.
D. Pursue risk acceptance for the slower response time.
Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 739
Which of the following is the **MOST** important influence to the continued success of an organization's information security strategy?

A. Information systems
B. Policy development

C. Security processes
D. Organizational culture

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 740
Which of the following metrics would be considered an accurate measure of an information security program's performance?

A. The number of key risk indicators (KRIs) identified, monitored, and acted upon
B. A combination of qualitative and quantitative trends that enable decision making
C. A single numeric score derived from various measures assigned to the security program
D. A collection of qualitative indicators that accurately measure security exceptions

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 741
Which of the following is the **BEST** indication that an information security control is no longer relevant?
A. Users regularly bypass or ignore the control.
B. The control does not support a specific business function.
C. IT management does not support the control.
D. Following the control costs the business more than not following it.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 742
When granting a vendor remote access to a system, which of the following is the **MOST** important consideration?

A. Session monitoring
B. Hard drive encryption
C. Multi-factor authentication
D. Password hashing

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 743
Which of the following is the **PRIMARY** reason to avoid alerting certain users of an upcoming penetration test?

A. To prevent exploitation by malicious parties
B. To aid in the success of the penetration
C. To evaluate detection and response capabilities
D. To reduce the scope and duration of the test

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 744
Which of the following metrics provides the **BEST** indication of the effectiveness of a security awareness campaign?

A. The number of reported security events
B. Quiz scores for users who took security awareness classes
C. User approval rating of security awareness classes
D. Percentage of users who have taken the courses

Correct Answer: A

Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 745
Which of the following is the **BEST** type of access control for an organization with employees who move between departments?

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

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 746
Which of the following is the **BEST** mechanism to prevent data loss in the event personal computing equipment is stolen or lost?

A. Data encryption
B. Remote access to device
C. Data leakage prevention (DLP)
D. Personal firewall

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 747
Using which of the following metrics will **BEST** help to determine the resiliency of IT infrastructure security controls?

A. Number of successful disaster recovery tests
B. Percentage of outstanding high-risk audit issues
C. Frequency of updates to system software
D. Number of incidents resulting in disruptions

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 748
An employee is found to be using an external cloud storage service to share corporate information with a third-party consultant, which is against company policy. Which of the following should be the information security manager's **FIRST** course of action?

A. Determine the classification level of the information.
B. Seek business justification from the employee.
C. Block access to the cloud storage service.
D. Inform higher management a security breach.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 749
Which of the following is the **MOST** important outcome of a well-implemented awareness program?

A. The board is held accountable for risk management.
B. The number of reported security incidents steadily decreases.
C. The number of successful social engineering attacks is reduced.
D. Help desk response time to resolve incidents is improved.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 750
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 751
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: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
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 752
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-life 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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 753
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 limitsC. User awareness training
D. Taking disciplinary action
Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
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 754
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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 755
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: INFORMATION SECURITY PROGRAM MANAGEMENT
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.

QUESTION 756
Which of the following BEST ensures timely and reliable access to services?

A. Authenticity
B. Recovery time objective
C. Availability
D. Nonrepudiation

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
Reference: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

QUESTION 757
Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is MOST important for the information security manager to periodically:

A. perform a cost-benefit analysis
B. review firewall configuration
C. review the security policy
D. perform a risk assessment

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 758
Which of the following is MOST difficult to achieve in a public cloud-computing environment?

A. Cost reduction
B. Pay per use
C. On-demand provisioning
D. Ability to audit

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 759
An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resource to support clients. The BEST approach to obtain the support of business unit management would be to:

A. present an analysis of the cost and benefit of the changes
B. discuss the risk and impact of security incidents if not implemented
C. present industry benchmarking results to business units
D. elaborate on the positive impact to information security

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 760
Ensuring that an organization can conduct security reviews within third-party facilities is **PRIMARILY** enabled by:

A. service level agreements (SLAs)
B. acceptance of the organization's security policies
C. contractual agreements
D. audit guidelines
Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 761
A contract bid is digitally signed and electronically mailed. The PRIMARY advantage to using a digital signature is that:

A. the bid and the signature can be copied from one document to another
B. the bid cannot be forged even if the keys are compromised

C. the signature can be authenticated even if no encryption is used
D. any alteration of the bid will invalidate the signature

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 762
An organization has purchased a security information and event management (SIEM) tool. Which of the following is **MOST** important to consider before implementation?

A. Reporting capabilities
B. The contract with the SIEM vendor
C. Controls to be monitored
D. Available technical support

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 763
Which of the following **BEST** enables an information security manager to communicate the capability of security program functions?

A. Security architecture diagrams
B. Security maturity assessments
C. Vulnerability scan results
D. Key risk indicators (KRIs)

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 764
Which of the following is the **PRIMARY** purpose for defining key performance indicators (KPIs) for a security program?

A. To compare security program effectiveness to best practice
B. To ensure controls meet regulatory requirements
C. To measure the effectiveness of the security program
D. To evaluate the performance of security staff

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 765
Which of the following is **MOST** appropriate to include in an information security policy?

A. A set of information security controls to maintain regulatory compliance
B. The strategy for achieving security program outcomes desired by management
C. A definition of minimum level of security that each system must meet
D. Statements of management's intent to support the goals of information security

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 766
Which of the following provides the **BEST** indication of strategic alignment between an organization's information security program and business objectives?

A. A business impact analysis (BIA)
B. Security audit reports
C. A balanced scorecard
D. Key risk indicators (KRIs)

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 767
Which of the following is the **BEST** way to define responsibility for information security throughout an organization?

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

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 768
Which of the following would **BEST** enable effective decision-making?

A. A consistent process to analyze new and historical information risk
B. Annualized loss estimates determined from past security events
C. Formalized acceptance of risk analysis by business management
D. A universally applied list of generic threats, impacts, and vulnerabilities

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 769

When a security weakness is detected at facilities provided by an IT service provider, which of the following tasks must the information security manager perform **FIRST**?

A. Assess compliance with the service provider's security policy.
B. Advise the service provider of countermeasures.
C. Confirm the service provider's contractual obligations.
D. Reiterate the relevant security policy and standards.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 770
An organization manages payroll and accounting systems for multiple client companies. Which of the following contract terms would indicate a potential weakness for a disaster recovery hot site?

A. Exclusive use of hot site is limited to six weeks (following declaration).
B. Timestamp of declaration will determine priority of access to facility.
C. Work-area size is limited but can be augmented with nearby office space.
D. Servers will be provided at time of disaster (not on floor).

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation
Explanation/Reference:

QUESTION 771
While conducting a test of a business continuity plan (BCP), which of the following is the **MOST** important consideration?

A. The test addresses the critical components.
B. The test simulates actual prime-time processing conditions.
C. The test is scheduled to reduce operational impact.
D. The test involves IT members in the test process.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 772
Which of the following is the **MOST** appropriate party to approve an information security strategy?

A. Executive leadership team
B. Chief information officer
C. Information security management committee
D. Chief information security officer

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 773
An application system stores customer confidential data and encryption is not practical. The **BEST** measure to protect against data disclosure is:

A. regular review of access logs.
B. single sign-on.
C. nondisclosure agreements (NDA).
D. multi-factor access controls.

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 774
The **BEST** way to establish a security baseline is by documenting:

A. the organization's preferred security level.
B. a framework of operational standards.
C. the desired range of security settings.
D. a standard of acceptable settings.

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 775
Presenting which of the following to senior management will be **MOST** helpful in securing ongoing support for the information security strategy?

A. Historical security incidents
B. Return on security investment
C. Completed business impact analyses (BIAs)
D. Current vulnerability metrics

Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:
QUESTION 776
From an information security perspective, legal issues associated with a transborder flow of technology-related items are **MOST** often related to:

A. website transactions and taxation.
B. lack of competition and free trade.
C. encryption tools and personal data.
D. software patches and corporate data.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 777
An organization has decided to store production data in a cloud environment. What should be the **FIRST** consideration?

A. Data backup
B. Data transfer
C. Data classification
D. Data isolation

Correct Answer: D
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 778
Which of the following factors are the **MAIN** reasons why large networks are vulnerable?

A. Hacking and malicious software
B. Connectivity and complexity
C. Network operating systems and protocols
D. Inadequate training and user errors
Correct Answer: B
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 779
While auditing a data center's IT architecture, an information security manager discovers that required encryption for data communications has not been implemented. Which of the following should be done **NEXT**?

A. Evaluate compensating and mitigating controls
B. Perform a cost benefit analysis.
C. Perform a business impact analysis (BIA).
D. Document and report the findings.

Correct Answer: C
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 780
When monitoring the security of a web-based application, which of the following is **MOST** frequently reviewed?

A. Access logs
B. Audit reports
C. Access lists
D. Threat metrics

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 781
Senior management is concerned a security solution may not adequately protect its multiple global data centers following recent industry breaches. What should be done **NEXT**?

A. Perform a gap analysis.
B. Conduct a business impact analysis (BIA).
C. Perform a risk assessment.
D. Require an internal audit review.

Correct Answer: A
Section: INFORMATION SECURITY PROGRAM MANAGEMENT
Explanation

Explanation/Reference:

QUESTION 782

An information security manager is analyzing a risk that is believed to be severe, but lacks numerical evidence to determine the impact the risk could have on the organization. In this case the information security manager should:

A. use a qualitative method to assess the risk.
B. use a quantitative method to assess the risk.
C. put it in the priority list in order to gain time to collect more data.
D. ask management to increase staff in order to collect more evidence on severity.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 783
An organization experienced a breach which was successfully contained and remediated. Based on industry regulations, the breach needs to be communicated externally. What should the information security manager do **NEXT**?

A. Refer to the incident response plan.
B. Send out a breach notification to all parties involved.
C. Contact the board of directors.
D. Invoke the corporate communications plan.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 784
Which of the following provides the **BEST** indication that the information security program is in alignment with enterprise requirements?

A. The security strategy is benchmarked with similar organizations.
B. The information security manager reports to the chief executive officer.
C. Security strategy objectives are defined in business terms.
D. An IT governance committee is in place.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 785
Which of the following is **MOST** critical when creating an incident response plan?

A. Identifying what constitutes an incident
B. Identifying vulnerable data assets
C. Aligning with the risk assessment process
D. Documenting incident notification and escalation processes

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:

QUESTION 786
Which of the following is the **MOST** effective way to detect security incidents?

A. Analyze penetration test results.
B. Analyze recent security risk assessments.
C. Analyze vulnerability assessments.
D. Analyze security anomalies.

Correct Answer: D

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 787
Following a successful and well-publicized hacking incident, an organization has plans to improve application security.

Which of the following is a security project risk?

A. Critical evidence may be lost.
B. The reputation of the organization may be damaged.
C. A trapdoor may have been installed in the application.
D. Resources may not be available to support the implementation.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 788
Establishing which of the following is the **BEST** way of ensuring that the emergence of new risk is promptly identified?

A. Regular risk reporting
B. Risk monitoring processes
C. Change control procedures
D. Incident monitoring activities

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 789

Which of the following metrics is **MOST** useful to demonstrate the effectiveness of an incident response plan?

A. Average time to resolve an incident
B. Total number of reported incidents
C. Total number of incident responses
D. Average time to respond to an incident

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 790
A global organization is developing an incident response team (IRT). The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events.

Which of the following IRT models **BEST** supports these objectives?

A. Holistic IRT
B. Central IRT
C. Coordinating IRT
D. Distributed IRT

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 791
The decision to escalate an incident should be based **PRIMARILY** on:

A. organizational hierarchy.
B. prioritization by the information security manager.
C. predefined policies and procedures.

D. response team experience.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 792
What is the **MOST** important factor for determining prioritization of incident response?

A. Service level agreements (SLAs) pertaining to the impacted systems
B. The potential impact to the business
C. The time to restore the impacted systems
D. The availability of specialized technical staff

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 793
When developing a classification method for incidents, the categories **MUST** be:

A. quantitatively defined.

B. regularly reviewed.
C. specific to situations.
D. assigned to incident handlers.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 794
The MAIN consideration when designing an incident escalation plan should be ensuring that:

A. appropriate stakeholders are involved
B. information assets are classified
C. requirements cover forensic analysis
D. high-impact risks have been identified

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 795
An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

A. Activate the organization's incident response plan
B. Include security requirements in outsourcing contracts
C. Terminate the agreement with the third-party contractor
D. Limit access to the third-party contractor

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 796
What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?

A. Establish and measure key performance indicators (KPIs)
B. Communicate incident response procedures to staff
C. Test incident response procedures regularly
D. Obtain senior management commitment

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 797
An information security manager is developing evidence preservation procedures for an incident response plan. Which of the following would be the BEST source of guidance for requirements associated with the procedures?

A. IT management
B. Legal counsel
C. Executive management
D. Data owners

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 798
Which of the following is the MOST beneficial outcome of testing an incident response plan?

A. Test plan results are documented
B. The plan is enhanced to reflect the findings of the test
C. Incident response time is improved
D. The response includes escalation to senior management

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 799

Following a malicious security incident, an organization has decided to prosecute those responsible. Which of the following will BEST facilitate the forensic investigation?

A. Performing a backup of affected systems
B. Identifying the affected environment
C. Maintaining chain of custody
D. Determining the degree of loss

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 800
Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?

A. Regulatory compliance
B. Business impact
C. Management support
D. Residual risk

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 801
Which is the **MOST** important to enable a timely response to a security breach?

A. Knowledge sharing and collaboration
B. Security event logging
C. Roles and responsibilities
D. Forensic analysis

Correct Answer: B

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 802
The **MOST** likely cause of a security information event monitoring (SIEM) solution failing to identify a serious incident is that the system:

A. is not collecting logs from relevant devices.
B. has not been updated with the latest patches.
C. is hosted by a cloud service provider.
D. has performance issues.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 803
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: INCIDENT MANAGEMENT AND RESPONSE
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 804
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 GREATEST 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: INCIDENT MANAGEMENT AND RESPONSE
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 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 805
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: INCIDENT MANAGEMENT AND RESPONSE
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 806
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

QUESTION 807
The FIRST priority when responding to a major security incident is:

A. documentation.
B. monitoring.
C. restoration.
D. containment.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
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 808
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: INCIDENT MANAGEMENT AND RESPONSE
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 809
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: INCIDENT MANAGEMENT AND RESPONSE
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 810

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: INCIDENT MANAGEMENT AND RESPONSE
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 811
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: INCIDENT MANAGEMENT AND RESPONSE
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 812
Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

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

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
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 813
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: INCIDENT MANAGEMENT AND RESPONSE
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 814
Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

A. Detailed technical recovery plans are maintained offsite

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
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 815
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: INCIDENT MANAGEMENT AND RESPONSE
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 816
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that it 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 817
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: INCIDENT MANAGEMENT AND RESPONSE
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.

QUESTION 818
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: INCIDENT MANAGEMENT AND RESPONSE
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 819
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: INCIDENT MANAGEMENT AND RESPONSE
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 820
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: INCIDENT MANAGEMENT AND RESPONSE
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 821
A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

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

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
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 822
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: INCIDENT MANAGEMENT AND RESPONSE
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 823
Isolation and containment measures for a compromised computer has 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: INCIDENT MANAGEMENT AND RESPONSE
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 824
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: INCIDENT MANAGEMENT AND RESPONSE
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 825
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: INCIDENT MANAGEMENT AND RESPONSE
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.

QUESTION 826
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: INCIDENT MANAGEMENT AND RESPONSE
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 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 827
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: INCIDENT MANAGEMENT AND RESPONSE
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 828
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: INCIDENT MANAGEMENT AND RESPONSE
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 829
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: INCIDENT MANAGEMENT AND RESPONSE
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 830
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:
Explanation:

Before performing analysis of impact, resolution, notification or isolation of an incident, it must be validated as a real security incident.

QUESTION 831
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: INCIDENT MANAGEMENT AND RESPONSE
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 832
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: INCIDENT MANAGEMENT AND RESPONSE
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 833
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: INCIDENT MANAGEMENT AND RESPONSE
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 834
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 835
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: INCIDENT MANAGEMENT AND RESPONSE
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 836
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: INCIDENT MANAGEMENT AND RESPONSE
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 837
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: INCIDENT MANAGEMENT AND RESPONSE
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.

QUESTION 838
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: INCIDENT MANAGEMENT AND RESPONSE
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 839
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: INCIDENT MANAGEMENT AND RESPONSE
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 review of these logs.

QUESTION 840
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: INCIDENT MANAGEMENT AND RESPONSE
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 841
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: INCIDENT MANAGEMENT AND RESPONSE
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 842
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
C. Vulnerability assessment
D. Business process mapping

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
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 843
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: INCIDENT MANAGEMENT AND RESPONSE
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 844
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: INCIDENT MANAGEMENT AND RESPONSE
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 845
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 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: INCIDENT MANAGEMENT AND RESPONSE
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 846
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: INCIDENT MANAGEMENT AND RESPONSE
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 847
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.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
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 848
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: INCIDENT MANAGEMENT AND RESPONSE
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 849
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: INCIDENT MANAGEMENT AND RESPONSE
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 850
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: INCIDENT MANAGEMENT AND RESPONSE
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 851
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: INCIDENT MANAGEMENT AND RESPONSE
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 852
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: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
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 853
Which of the following recovery strategies has the GREATEST chance of failure?

A. Hot site
B. Redundant site
C. Reciprocal arrangement
D. Cold site

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
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 854
Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

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

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
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 855
In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized
B. Managed

C. Defined
D. Repeatable
Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

QUESTION 856
When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

QUESTION 857
An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A. A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
B. Firewall policies are updated on the basis of changing requirements.
C. Inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all installation options.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

QUESTION 858
Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
Explanation:
When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

QUESTION 859
When segregation of duties concerns exists between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:
Explanation:
Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

QUESTION 860
When training an incident response team, the advantage of using tabletop exercises is that they:

A. provide the team with practical experience in responding to incidents
B. ensure that the team can respond to any incident
C. remove the need to involve senior managers in the response process
D. enable the team to develop effective response interactions

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 861
Which of the following is the PRIMARY objective of incident classification?

A. Complying with regulatory requirements
B. Increasing response efficiency
C. Enabling incident reporting
D. Reducing escalations to management

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 862
Which of the following activities is used to determine the effect of a disruptive event?

A. Maximum tolerable downtime assessment
B. Recovery time objective (RTO) analysis
C. Business impact analysis (BIA)
D. Incident impact analysis

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 863
For an organization that provides web-based services, which of the following security events would **MOST** likely initiate an incident response plan and be escalated to management?

A. Multiple failed login attempts on an employee's workstation
B. Suspicious network traffic originating from the demilitarized zone (DMZ)
C. Several port scans of the web server
D. Anti-malware alerts on several employees' workstations

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 864
Which of the following is the **MOST** reliable way to ensure network security incidents are identified as soon as possible?

A. Collect and correlate IT infrastructure event logs.
B. Conduct workshops and training sessions with end users.

C. Install stateful inspection firewalls.
D. Train help desk staff to identify and prioritize security incidents.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 865
Which of the following would be **MOST** helpful to reduce the amount of time needed by an incident response team to determine appropriate actions?

A. Providing annual awareness training regarding incident response for team members
B. Defining incident severity levels during a business impact analysis (BIA)
C. Validating the incident response plan against industry best practices
D. Rehearsing incident response procedures, roles, and responsibilities

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 866
Which of the following is the **BEST** way for an organization to ensure that incident response teams are properly prepared?

A. Conducting tabletop exercises appropriate for the organization
B. Providing training from third-party forensics firms
C. Documenting multiple scenarios for the organization and response steps
D. Obtaining industry certifications for the response team

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 867
The **MOST** important reason to have a well-documented and tested incident response plan in place is to:

A. standardize the chain of custody procedure
B. facilitate the escalation process
C. promote a coordinated effort.
D. outline external communications

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 868
Which of the following helps to ensure that the appropriate resources are applied in a timely manner after an incident has occurred?

A. Initiate an incident management log.
B. Define incident response teams.
C. Broadcast an emergency message.
D. Classify the incident.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 869
After a server has been attacked, which of the following is the **BEST** course of action?

A. Conduct a security audit
B. Review vulnerability assessment
C. Isolate the system
D. Initiate incident response

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 870
An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do **FIRST**?

A. Disable remote access
B. Initiate a device reset
C. Initiate incident response
D. Conduct a risk assessment

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 871
An organization experienced a data breach and followed its incident response plan. Later it was discovered that the plan was incomplete, omitting a requirement to report the incident to the relevant authorities. In addition to establishing an updated incident response plan, which of the following would be **MOST** helpful in preventing a similar occurrence?

A. Attached reporting forms as an addendum to the incident response plan
B. Management approval of the incident reporting process
C. Ongoing evaluation of the incident response plan.
D. Assignment of responsibility for communications.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 872

An audit has determined that employee use of personal mobile devices to access the company email system is resulting in confidential data leakage. The information security manager's **FIRST** course of action should be to:

A. treat the situation as a security incident to determine appropriate response
B. implement a data leakage prevention tool to stem further loss.
C. isolate the mobile devices on the network for further investigation.
D. treat the situation as a new risk and update the security risk register.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 873
Which of the following is the **MOST** important criterion for complete closure of a security incident?

A. Level of potential impact
B. Root-cause analysis and lessons learned
C. Identification of affected resources
D. Documenting and reporting to senior management

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 874
Which of the following is the **MOST** effective way to detect information security incidents?

A. Providing regular and up-to-date training for the incident response team
B. Establishing proper policies for response to threats and vulnerabilities
C. Performing regular testing of the incident response program
D. Educating and users on threat awareness and timely reporting

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 875
Which of the following is **MOST** important to verify when reviewing the effectiveness of response to an information security incident?

A. Lessons learned have been implemented.
B. Testing has been completed on time.
C. Test results have been properly recorded.
D. Metrics have been captured in a dashboard.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 876
Which of the following is a security manager's **FIRST** priority after an organization's critical system has been compromised?

A. Implement improvements to prevent recurrence.
B. Restore the compromised system.
C. Preserve incident-related data.
D. Identify the malware that compromised the system.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 877
The **PRIMARY** focus of a training curriculum for members of an incident response team should be:

A. specific role training

B. external corporate communication
C. security awareness
D. technology training
Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 878
The **BEST** way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. results of exit interviews
B. previous training sessions.
C. examples of help desk requests.
D. responses to security questionnaires.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 879
Which of the following is **MOST** important for the effectiveness of an incident response function?

A. Enterprise security management system and forensic tools.
B. Establishing prior contacts with law enforcement
C. Training of all users on when and how to report
D. Automated incident tracking and reporting tools

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 880
Which of the following is the **PRIMARY** responsibility of the designated spokesperson during incident response testing?
A. Communicating the severity of the incident to the board
B. Establishing communication channels throughout the organization
C. Evaluating the effectiveness of the communication processes
D. Acknowledging communications from the incident response team

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 881
Which of the following **BEST** contributes to the successful management of security incidents?

A. Established procedures
B. Established policies
C. Tested controls
D. Current technologies

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 882
It is suspected that key e-mails have been viewed by unauthorized parties. The e-mail administrator conducted an investigation but it has not returned any information relating to the incident, and leaks are continuing. Which of the following is the **BEST** recommended course of action to senior management?

A. Commence security training for staff at the organization.
B. Arrange for an independent review.
C. Rebuild the e-mail application.
D. Restrict the distribution of confidential e-mails.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 883
Which of the following **BEST** prepares a computer incident response team for a variety of information security scenarios?

A. Tabletop exercises
B. Forensics certification
C. Penetration tests
D. Disaster recovery drills

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 884
Who is **MOST** important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data loss?

A. An independent auditor for identification of control deficiencies
B. A damage assessment expert for calculating losses
C. A forensics expert for evidence management
D. A penetration tester to validate the attack

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 885

When an information security manager presents an information security program status report to senior management, the **MAIN** focus should be:

A. critical risks indicators.

B. key controls evaluation.
C. key performance indicators (KPIs).
D. net present value (NPV).

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 886
Reviewing which of the following would provide the **GREATEST** input to the asset classification process?

A. Risk assessment
B. Replacement cost of the asset
C. Sensitivity of the data
D. Compliance requirements

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 887
Which of the following should be an information security manager's **MOST** important concern to ensure admissibility of information security evidence from cyber crimes?

A. Chain of custody
B. Tools used for evidence analysis
C. Forensics contractors
D. Efficiency of the forensics team

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:

QUESTION 888
Which of the following information security metrics is the **MOST** difficult to quantify?

A. Cost of security incidents prevented
B. Percentage of controls mapped to industry frameworks
C. Extent of employee security awareness
D. Proportion of control costs to asset value

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 889
Which of the following is the **BEST** method to ensure that data owners take responsibility for implementing information security processes?

A. Include security tasks into employee job descriptions.
B. Include membership on project teams.
C. Provide job rotation into the security organization.
D. Increase security awareness training.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 890
Which of the following is the **MAIN** benefit of performing an assessment of existing incident response processes?

A. Identification of threats and vulnerabilities
B. Prioritization of action plans
C. Validation of current capabilities
D. Benchmarking against industry peers

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 891
Which of the following has the **GREATEST** influence on an organization's information security strategy?

A. The organization's risk tolerance
B. The organizational structure
C. Information security awareness
D. Industry security standards

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 892
The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do **NEXT**?

A. Formally document the decision.
B. Review the risk monitoring plan.
C. Perform a risk reassessment.
D. Implement the recommendations.

Correct Answer: A

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 893
To integrate security into system development life cycle (SDLC) processes, an organization **MUST** ensure that security:

A. is represented on the configuration control board.
B. performance metrics have been met.
C. roles and responsibilities have been defined.
D. is a prerequisite for completion of major phases.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 894
When facilitating the alignment of corporate governance and information security governance, which of the following is the **MOST** important role of an organization's security steering committee?

A. Obtaining support for the integration from business owners
B. Defining metrics to demonstrate alignment
C. Obtaining approval for the information security budget
D. Evaluating and reporting the degree of integration

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 895
Which of the following is the **PRIMARY** purpose of establishing an information security governance framework?

A. To minimize security risks

B. To proactively address security objectives
C. To reduce security audit issues
D. To enhance business continuity planning
Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 896
Which of the following should be done **FIRST** when handling multiple confirmed incidents raised at the same time?

A. Activate the business continuity plan (BCP).
B. Update the business impact assessment.
C. Inform senior management.
D. Categorize incidents by the value of the affected asset.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 897
Which of the following **BEST** enables a more efficient incident reporting process?

A. Training executive management for communication with external entities
B. Educating the incident response team on escalation procedures
C. Educating IT teams on compliance requirements
D. Training end users to identify abnormal events

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 898
Which of the following is **MOST** important for effective communication during incident response?
A. Maintaining a relationship with media and law enforcement
B. Maintaining an updated contact list
C. Establishing a recovery time objective (RTO)
D. Establishing a mean time to resolve (MTTR) metric

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 899
An information security manager is reviewing the organization's incident response policy affected by a proposed public cloud integration. Which of the following will be the **MOST** difficult to resolve with the cloud service provider?

A. Accessing information security event data
B. Regular testing of incident response plan
C. Obtaining physical hardware for forensic analysis
D. Defining incidents and notification criteria

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 900
Which of the following is the **PRIMARY** goal of an incident response team during a security incident?

A. Ensure the attackers are detected and stopped
B. Minimize disruption to business-critical operations
C. Maintain a documented chain of evidence
D. Shut down the affected systems to limit the business impact

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:

QUESTION 901
Which of the following techniques is **MOST** useful when an incident response team needs to respond to external attacks on multiple corporate network devices?

A. Penetration testing of network devices
B. Vulnerability assessment of network devices
C. Endpoint baseline configuration analysis
D. Security event correlation analysis

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 902
The head of a department affected by a recent security incident expressed concern about not being aware of the actions taken to resolve the incident. Which of the following is the **BEST** way to address this issue?

A. Ensure better identification of incidents in the incident response plan.
B. Discuss the definition of roles in the incident response plan.
C. Require management approval of the incident response plan.
D. Disseminate the incident response plan throughout the organization.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 903
When responding to an incident, which of the following is required to ensure evidence remains legally admissible in court?

A. Law enforcement oversight
B. Chain of custody
C. A documented incident response plan
D. Certified forensics examiners

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 904
Which of the following provides the **BEST** opportunity to evaluate the capabilities of incident response team members?

A. Disaster recovery exercise
B. Black box penetration test
C. Breach simulation exercise
D. Tabletop test

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 905
The **PRIMARY** reason for implementing scenario-based training for incident response is to:

A. help incident response team members understand their assigned roles.
B. verify threats and vulnerabilities faced by the incident response team.
C. ensure staff knows where to report in the event evacuation is required.
D. assess the timeliness of the incident team response and remediation.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 906

What should be an information security manager's **PRIMARY** objective in the event of a security incident?

A. Contain the threat and restore operations in a timely manner.
B. Ensure that normal operations are not disrupted.
C. Identify the source of the breach and how it was perpetrated.
D. Identify lapses in operational control effectiveness.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 907

Which of the following should be the **FIRST** step of incident response procedures?

A. Classify the event depending on severity and type.
B. Identify if there is a need for additional technical assistance.
C. Perform a risk assessment to determine the business impact.
D. Evaluate the cause of the control failure.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 908

What should an information security manager do **FIRST** when a service provider that stores the organization's confidential customer data experiences a breach in its data center?

A. Engage an audit of the provider's data center.
B. Recommend canceling the outsourcing contract.
C. Apply remediation actions to counteract the breach.

D. Determine the impact of the breach.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 909
Which of the following is **MOST** critical for responding effectively to security breaches?

A. Root cause analysis
B. Evidence gathering
C. Management communication
D. Counterattack techniques

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 910
What should be an information security manager's **FIRST** course of action upon learning of a security threat that has occurred in the industry for the first time?

A. Update the relevant information security policy.
B. Perform a control gap analysis of the organization's environment.
C. Revise the organization's incident response plan.
D. Examine responses of victims that have been exposed to similar threats.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 911
Which of the following would **BEST** help to ensure the alignment between information security and business functions?

A. Establishing an information security governance committee
B. Developing information security policies
C. Providing funding for information security efforts
D. Establishing a security awareness program

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 912
When designing security controls, it is **MOST** important to:

A. apply a risk-based approach.
B. focus on preventive controls.
C. evaluate the costs associated with the controls.
D. apply controls to confidential information.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 913
Which of the following should be the **MOST** important consideration of business continuity management?

A. Ensuring human safety
B. Identifying critical business processes
C. Ensuring the reliability of backup data
D. Securing critical information assets

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 914
Which of the following would be **MOST** helpful when justifying the funding required for a compensating control?

A. Business case
B. Risk analysis
C. Business impact analysis
D. Threat assessment

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 915
Which of the following would **MOST** effectively ensure that information security is implemented in a new system?

A. Security baselines
B. Security scanning
C. Secure code reviews
D. Penetration testing

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 916

A penetration test was conducted by an accredited third party. Which of the following should be the information security manager's **FIRST** course of action?

A. Ensure vulnerabilities found are resolved within acceptable timeframes.

B. Request funding needed to resolve the top vulnerabilities.
C. Report findings to senior management.
D. Ensure a risk assessment is performed to evaluate the findings.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 917
Which of the following is the **MOST** important consideration when establishing an information security governance framework?

A. Security steering committee meetings are held at least monthly.
B. Members of the security steering committee are trained in information security.
C. Business unit management acceptance is obtained.
D. Executive management support is obtained.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 918
Which of the following is the **MOST** effective approach for delivering security incident response training?

A. Perform role-playing exercises to simulate real-world incident response scenarios.
B. Engage external consultants to present real-world examples within the industry.
C. Include incident response training within new staff orientation.
D. Provide on-the-job training and mentoring for the incident response team.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 919
An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is **MOST** important to:

A. prohibit remote access to the site.
B. periodically recertify access rights.
C. enforce document lifecycle management.
D. conduct a vulnerability assessment.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 920
A large number of exceptions to an organization's information security standards have been granted after senior management approved a bring your own device (BYOD) program. To address this situation, it is **MOST** important for the information security manager to:

A. introduce strong authentication on devices.
B. reject new exception requests.
C. update the information security policy.
D. require authorization to wipe lost devices.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 921
An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The **PRIMARY** purpose of this analysis should be to:

A. prepare for criminal prosecution.
B. document lessons learned.
C. evaluate the impact.
D. update information security policies.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 922
When developing a new system, detailed information security functionality should **FIRST** be addressed:

A. as part of prototyping.
B. during the system design phase.
C. when system requirements are defined.
D. as part of application development.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 923
An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:

A. mobile device configuration.
B. asset management guidelines.
C. the business impact analysis (BIA).
D. incident classification.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 924

Senior management wants to provide mobile devices to its sales force. Which of the following should the information security manager do **FIRST** to support this objective?

A. Assess risks introduced by the technology.
B. Develop an acceptable use policy.
C. Conduct a vulnerability assessment on the devices.
D. Research mobile device management (MDM) solutions.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 925

An information security manager discovers that newly hired privileged users are not taking necessary steps to protect critical information at their workstations. Which of the following is the **BEST** way to address this situation?

A. Communicate the responsibility and provide appropriate training.
B. Publish an acceptable use policy and require signed acknowledgment.
C. Turn on logging and record user activity.
D. Implement a data loss prevention (DLP) solution.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 926

The **BEST** way to minimize errors in the response to an incident is to:

A. follow standard operating procedures.
B. analyze the situation during the incident.

C. implement vendor recommendations.
D. reference system administration manuals.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 927
The **PRIMARY** goal of a security infrastructure design is the:

A. reduction of security incidents.
B. protection of corporate assets.
C. elimination of risk exposures.
D. optimization of IT resources.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 928
When outsourcing information security administration, it is **MOST** important for an organization to include:

A. nondisclosure agreements (NDAs)
B. contingency plans
C. insurance requirements
D. service level agreements (SLAs)

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 929
Who should determine data access requirements for an application hosted at an organization's data center?

A. Business owner
B. Information security manager
C. Systems administrator
D. Data custodian

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 930
When conducting a post-incident review, the **GREATEST** benefit of collecting mean time to resolution (MTTR) data is the ability to:

A. reduce the costs of future preventive controls.
B. provide metrics for reporting to senior management.
C. learn of potential areas of improvement.
D. verify compliance with the service level agreement (SLA).

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 931
Which of the following provides the **MOST** relevant information to determine the overall effectiveness of an information security program and underlying business processes?

A. Balanced scorecard
B. Cost-benefit analysis
C. Industry benchmarks
D. SWOT analysis

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 932
Which of the following is the **FIRST** step to perform before outsourcing critical information processing to a third party?

A. Require background checks for third-party employees.
B. Perform a risk assessment.
C. Ensure that risks are formally accepted by third party.
D. Negotiate a service level agreement.

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 933
Which of the following should occur **FIRST** in the process of managing security risk associated with the transfer of data from unsupported legacy systems to supported systems?

A. Make backups of the affected systems prior to transfer.
B. Increase cyber insurance coverage.
C. Identify all information assets in the legacy environment.
D. Assign owners to be responsible for the transfer of each asset.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 934

When reviewing the security controls of an application service provider, an information security manager discovers the provider's change management controls are insufficient. Changes to the provided application often occur spontaneously with no notification to clients. Which of the following would **BEST** facilitate a decision to continue or discontinue services with this provider?

A. Comparing the client organization's risk appetite to the disaster recovery plan of the service provider.
B. Comparing the client organization's risk appetite to the criticality of the supplied application. C. Comparing the client organization's risk appetite to the frequency of application downtimes.
D. Comparing the client organization's risk appetite to the vendor's change control policy.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 935
Which of the following would provide the **MOST** essential input for the development of an information security strategy?

A. Measurement of security performance against IT goals
B. Results of an information security gap analysis
C. Availability of capable information security resources
D. Results of a technology risk assessment

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 936
Which of the following is a **PRIMARY** security responsibility of an information owner?

A. Deciding what level of classification the information requires
B. Testing information classification controls
C. Maintaining the integrity of data in the information system
D. Determining the controls associated with information classification

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 937
When implementing a new risk assessment methodology, which of the following is the **MOST** important requirement?

A. Risk assessments must be conducted by certified staff.
B. The methodology must be approved by the chief executive officer.
C. Risk assessments must be reviewed annually.
D. The methodology used must be consistent across the organization.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 938
Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

A. Corresponding breaches associated with each vendor
B. Compensating controls in place to protect information security
C. Compliance requirements associated with the regulation
D. Criticality of the service to the organization

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 939

An organization performed a risk analysis and found a large number of assets with low-impact vulnerabilities. The **NEXT** action of the information security manager should be to:

A. determine appropriate countermeasures.
B. transfer the risk to a third party.
C. report to management.
D. quantify the aggregated risk.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 940
What is the **PRIMARY** goal of an incident management program?

A. Minimize impact to the organization.
B. Contain the incident.
C. Identify root cause.
D. Communicate to external entities.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 941
What information is **MOST** helpful in demonstrating to senior management how information security governance aligns with business objectives?

A. Updates on information security projects in development
B. Drafts of proposed policy changes
C. Metrics of key information security deliverables
D. A list of monitored threats, risks, and exposures

Correct Answer: C

Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation
Explanation/Reference:

QUESTION 942
Which of the following would be of **GREATEST** assistance in determining whether to accept residual risk of a critical security system?

A. Maximum tolerable outage (MTO)
B. Cost-benefit analysis of mitigating controls
C. Annual loss expectancy (ALE)
D. Approved annual budget

Correct Answer: B
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 943
What should be the **PRIMARY** basis for prioritizing incident containment?

A. Legal and regulatory requirements
B. The recovery cost of affected assets
C. The business value of affected assets
D. Input from senior management

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 944
The **MOST** important reason to maintain metrics for incident response activities is to:

A. ensure that evidence collection and preservation are standardized.

B. prevent incidents from reoccurring.
C. support continual process improvement.
D. analyze security incident trends.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 945
The **PRIMARY** objective of periodically testing an incident response plan should be to:

A. highlight the importance of incident response and recovery.
B. harden the technical infrastructure.
C. improve internal processes and procedures.
D. improve employee awareness of the incident response process.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 946
The **MOST** effective way to determine the resources required by internal incident response teams is to:

A. test response capabilities with event scenarios.
B. determine the scope and charter of incident response.
C. request guidance from incident management consultants.
D. benchmark against other incident management programs.

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 947
An incident was detected where customer records were altered without authorization. The **GREATEST** concern for forensic analysis would be that the log data:

A. has been disclosed.
B. could be temporarily available.
C. may not be time-synchronized.
D. may be modified.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 948
Which of the following is the **MAIN** objective of classifying a security incident as soon as it is discovered?

A. Engaging appropriate resources
B. Enabling appropriate incident investigation
C. Downgrading the impact of the incident
D. Preserving relevant evidence

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 949
Which of the following is **MOST** important to help ensure an intrusion prevention system (IPS) can view all traffic in a demilitarized zone (DMZ)?

A. All internal traffic is routed to the IPS.
B. Connected devices can contact the IPS.
C. The IPS is placed outside of the firewall.

D. Traffic is decrypted before processing by the IPS.

Correct Answer: D
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 950
Which of the following is the **BEST** method to protect against data exposure when a mobile device is stolen?

A. Remote wipe capability
B. Password protection
C. Insurance
D. Encryption

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 951
Which of the following is **MOST** helpful in protecting against hacking attempts on the production network?

A. Intrusion prevention systems (IPSs)
B. Network penetration testing
C. Security information and event management (SIEM) tools
D. Decentralized honeypot networks

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 952
An information security manager has discovered an external break-in to the corporate network. Which of the following actions should be taken **FIRST**?

A. Switch on trace logging.

B. Copy event logs to a different server.
C. Isolate the affected portion of the network.
D. Shut down the network.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 953
Which of the following is **MOST** important for an information security manager to verify when selecting a third-party forensics provider?

A. Technical capabilities of the provider
B. Existence of the provider's incident response plan
C. Results of the provider's business continuity tests
D. Existence of a right-to-audit clause

Correct Answer: A
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:

QUESTION 954
An online trading company discovers that a network attack has penetrated the firewall. What should be the information security manager's **FIRST** response?

A. Notify the regulatory agency of the incident
B. Evaluate the impact to the business.
C. Implement mitigating controls
D. Examine firewall logs to identify the attacker.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference:
QUESTION 955
Which of the following is an organization's **BEST** approach for media communications when experiencing a disaster?

A. Defer public comment until partial recovery has been achieved.
B. Report high-level details of the losses and recovery strategy to the media.
C. Authorize a qualified representative to convey specially drafted messages.
D. Hold a press conference and advise the media to refer to legal authorities.

Correct Answer: C
Section: INCIDENT MANAGEMENT AND RESPONSE
Explanation

Explanation/Reference: