Isaca CISM

Certified Information Security Manager

Version: 15.0

Topic 1, INFORMATION SECURITY GOVERNANCE

QUESTION NO: 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

Answer: B
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 NO: 2

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

A.
use illustrative examples of successful attacks.

B.
explain the technical risks to the organization.

C.
evaluate the organization against best security practices.

D.
tie security risks to key business objectives.

Answer: D

Explanation:

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

QUESTION NO: 3

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

A.
evaluation of vendors offering security products.

B.
assessment of risks to the organization.

C.
approval of policy statements and funding.

D.
monitoring adherence to regulatory requirements.

Answer: C

Explanation:

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

QUESTION NO: 4

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

A.
Steering committees approve security projects

B.
Security policy training provided to all managers

C.
Security training available to all employees on the intranet

D.
Steering committees enforce compliance with laws and regulations

Answer: A
Explanation:

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

QUESTION NO: 5

Information security governance is PRIMARILY driven by:

A.
technology constraints.

B.
regulatory requirements.

C.
litigation potential.

D.
business strategy.

Answer: D

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 NO: 6

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

A.
Unrestricted data mining

B.
Identity theft

C.
Human rights protection

D.
Identifiable personal data

Answer: D

Explanation:

Protection of identifiable personal data is the major focus of recent privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Data mining is an accepted tool for ad hoc reporting; it could pose a threat to privacy only if it violates 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 NO: 7

Investments in information security technologies should be based on:

A.

vulnerability assessments.

B.
value analysis.

C.
business climate.

D.
audit recommendations.

Answer: B
Explanation:

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

QUESTION NO: 8

Retention of business records should PRIMARILY be based on:

A.
business strategy and direction.

B.
regulatory and legal requirements.

C.
storage capacity and longevity.

D.
business ease and value analysis.

Answer: B
Explanation:

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

QUESTION NO: 9

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

A.
More expensive to administer

B.
Better adherence to policies

C.
More aligned with business unit needs

D.
Faster turnaround of requests

Answer: B
Explanation:

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

QUESTION NO: 10

Successful implementation of information security governance will FIRST require:

A.
security awareness training.

B.
updated security policies.

C.
a computer incident management team.

D.
a security architecture.

Answer: B
Explanation:

Updated security policies are required to align management objectives with security procedures; management objectives translate into policy; policy translates into procedures. Security procedures will necessitate specialized teams such as the computer incident response and management group as well as specialized tools such as the security mechanisms that comprise the security architecture. Security awareness will promote the policies, procedures and appropriate use of the security mechanisms.

QUESTION NO: 11

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

Answer: B
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 NO: 12

The MOST important component of a privacy policy is:

A.
notifications.

B.
warranties.

C.
liabilities.

D.
geographic coverage.

Answer: A
Explanation:

Privacy policies must contain notifications and opt-out provisions: they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

QUESTION NO: 13

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

A.
annualized loss expectancy.

B.
cost of an incident.

C.
asset value.

D.
implementation opportunity costs.

Answer: C

Explanation:

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

QUESTION NO: 14

When a security standard conflicts with a business objective, the situation should be resolved by:

A.
changing the security standard.

B.
changing the business objective.

C.
performing a risk analysis.

D.
authorizing a risk acceptance.

Answer: C
Explanation:

Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. It is highly improbable that a business objective could be changed to accommodate a security standard, while risk acceptance* is a process that derives from the risk analysis.

QUESTION NO: 15

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

A.

strategy.

B.
guidelines.

C.
model.

D.
architecture.

Answer: D
Explanation:

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

QUESTION NO: 16

Which of the following is MOST appropriate for inclusion in an information security strategy?

A.
Business controls designated as key controls

B.
Security processes, methods, tools and techniques

C.
Firewall rule sets, network defaults and intrusion detection system (IDS) settings

D.
Budget estimates to acquire specific security tools

Answer: B
Explanation:

A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to periodic change, and are not appropriate content for a strategy document.

QUESTION NO: 17

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.

Answer: A
Explanation:

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

QUESTION NO: 18

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

A.
Evaluation of third parties requesting connectivity

B.
Assessment of the adequacy of disaster recovery plans

C.
Final approval of information security policies

D.
Monitoring adherence to physical security controls

Answer: C
Explanation:

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

QUESTION NO: 19

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.

Answer: D
Explanation:

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

QUESTION NO: 20

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

A.
Technical

B.
Regulatory

C.
Privacy

D.
Business

Answer: A
Explanation:

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

QUESTION NO: 21

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

A.
Develop a security architecture

B.

Establish good communication with steering committee members

C.
Assemble an experienced staff

D.
Benchmark peer organizations

Answer: B
Explanation:

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

QUESTION NO: 22

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

A.
Industry best practices

B.
Information technology plans

C.
Information security best practices

D.
Business objectives and goals

Answer: D
Explanation:

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

QUESTION NO: 23

Which of the following is MOST likely to be discretionary?

A.
Policies

B.
Procedures

C.
Guidelines

D.
Standards

Answer: C
Explanation:

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

QUESTION NO: 24

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.

Answer: A

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 NO: 25

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

A.
Standards

B.
Procedures

C.
Policies

D.
Guidelines

Answer: C

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 NO: 26

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.

Answer: D
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 NO: 27

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

A.
More uniformity in quality of service

B.
Better adherence to policies

C.
Better alignment to business unit needs

D.
More savings in total operating costs

Answer: C
Explanation:

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

QUESTION NO: 28

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

A.
Chief security officer (CSO)

B.
Chief operating officer (COO)

C.
Chief privacy officer (CPO)

D.
Chief legal counsel (CLC)

Answer: B
Explanation:

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

QUESTION NO: 29

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

A.
Review of internal control mechanisms

B.
Effective involvement in business decision making

C.
Total elimination of risk factors

D.
Ensuring trust in data

Answer: D
Explanation:

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

QUESTION NO: 30

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

A.
Security metrics

B.
Network topology

C.
Security architecture

D.
Process improvement models

Answer: C
Explanation:

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

QUESTION NO: 31

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

Answer: C
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 NO: 32

Acceptable levels of information security risk should be determined by:

A.
legal counsel.

B.
security management.

C.
external auditors.

D.
die steering committee.

Answer: D
Explanation:

Senior management, represented in the steering committee, has ultimate responsibility for determining what levels of risk the organization is willing to assume. Legal counsel, the external auditors and security management are not in a position to make such a decision.

QUESTION NO: 33

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

A.
establish security metrics and performance monitoring.

B.
educate business process owners regarding their duties.

C.
ensure that legal and regulatory requirements are met

D.
support the business objectives of the organization.

Answer: D
Explanation:

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

QUESTION NO: 34

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

A.
a formal security policy sponsored by the chief executive officer (CEO).

B.
regular security awareness training for employees.

C.
periodic review of alignment with business management goals.

D.
senior management signoff on the information security strategy.

Answer: C
Explanation:

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

QUESTION NO: 35

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

A.
Create separate policies to address each regulation

B.
Develop policies that meet all mandated requirements

C.
Incorporate policy statements provided by regulators

D.
Develop a compliance risk assessment

Answer: B
Explanation:

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

QUESTION NO: 36

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

A.
Interviewing candidates for information security specialist positions

B.
Developing content for security awareness programs

C.
Prioritizing information security initiatives

D.
Approving access to critical financial systems

Answer: C

Explanation:

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

QUESTION NO: 37

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

A.
Technical platform interfaces

B.
Scalability of the network

C.
Development methodologies

D.
Stakeholder requirements

Answer: D
Explanation:

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

QUESTION NO: 38

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

A.
Knowledge of information technology platforms, networks and development methodologies

B.
Ability to understand and map organizational needs to security technologies

C.
Knowledge of the regulatory environment and project management techniques

D.
Ability to manage a diverse group of individuals and resources across an organization

Answer: B
Explanation:

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

QUESTION NO: 39

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

A.
Procedures for hardening database servers

B.
Standards for password length and complexity

C.
Policies addressing information security governance

D.
Standards for document retention and destruction

Answer: A
Explanation:

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

QUESTION NO: 40

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

A.
Data owners

B.
Business process owners

C.
The security steering committee

D.
Security administrators

Answer: D

Explanation:

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

QUESTION NO: 41

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

A.
head of internal audit.

B.
chief operations officer (COO).

C.
chief technology officer (CTO).

D.
legal counsel.

Answer: B

Explanation:

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

QUESTION NO: 42

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

A.
Update platform-level security settings

B.
Conduct disaster recovery test exercises

C.
Approve access to critical financial systems

D.
Develop an information security strategy paper

Answer: D
Explanation:

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

QUESTION NO: 43

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

A.
assessing the frequency of incidents.

B.
quantifying the cost of control failures.

C.
calculating return on investment (ROI) projections.

D.
comparing spending against similar organizations.

Answer: C
Explanation:

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

QUESTION NO: 44

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.

Answer: D
Explanation:

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

QUESTION NO: 45

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

A.
Information security staffing requirements

B.

Current state and desired future state

C.
IT capital investment requirements

D.
information security mission statement

Answer: B
Explanation:

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

QUESTION NO: 46

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.

Answer: B
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 NO: 47

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

A.
Creation date

B.
Author name

C.
Initial draft approval date

D.
Last review date

Answer: D
Explanation:

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

QUESTION NO: 48

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

A.
Assign an information security administrator as regulatory liaison

B.
Perform self-assessments using regulatory guidelines and reports

C.
Assess previous regulatory reports with process owners input

D.
Ensure all regulatory inquiries are sanctioned by the legal department

Answer: B

Explanation:

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

QUESTION NO: 49

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

A.
bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.

B.
establish baseline standards for all locations and add supplemental standards as required.

C.
bring all locations into conformity with a generally accepted set of industry best practices.

D.
establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Answer: B
Explanation:

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

QUESTION NO: 50

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

Answer: B
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 NO: 51

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

A.
Enhanced policy compliance

B.
Improved procedure flows

C.
Segregation of duties

D.
Better accountability

Answer: D

Explanation:

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

QUESTION NO: 52

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

A.
Security metrics reports

B.
Risk assessment reports

C.
Business impact analysis (BIA)

D.
Return on security investment report

Answer: B

Explanation:

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

QUESTION NO: 53

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

A.
Risk assessment policies

B.
Return on security investment

C.
Security metrics

D.
User access rights

Answer: C
Explanation:

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

QUESTION NO: 54

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

Answer: C
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 NO: 55

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.

Answer: C
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 NO: 56

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.

Answer: A
Explanation:

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

QUESTION NO: 57

Information security policy enforcement is the responsibility of the:

A.
security steering committee.

B.
chief information officer (CIO).

C.
chief information security officer (CISO).

D.
chief compliance officer (CCO).

Answer: C
Explanation:

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

QUESTION NO: 58

A good privacy statement should include:

A.
notification of liability on accuracy of information.

B.
notification that information will be encrypted.

C.
what the company will do with information it collects.

D.
a description of the information classification process.

Answer: C
Explanation:

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

QUESTION NO: 59

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

A.
Regular password audits

B.
Single sign-on system

C.
Security awareness program

D.
Penalties for noncompliance

Answer: C

Explanation:

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

QUESTION NO: 60

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.

Answer: C

Explanation:

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

QUESTION NO: 61

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

A.
corporate data privacy policy.

B.
data privacy policy where data are collected.

C.
data privacy policy of the headquarters' country.

D.
data privacy directive applicable globally.

Answer: B
Explanation:

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

QUESTION NO: 62

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.

Answer: C

Explanation:

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

QUESTION NO: 63

The PRIMARY objective of a security steering group is to:

A.
ensure information security covers all business functions.

B.
ensure information security aligns with business goals.

C.
raise information security awareness across the organization.

D.
implement all decisions on security management across the organization.

Answer: B

Explanation:

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

QUESTION NO: 64

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

A.
baseline.

B.
strategy.

C.
procedure.

D.
policy.

Answer: D

Explanation:

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

QUESTION NO: 65

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

A.
When requested

B.
At testing

C.
At programming

D.
At detail requirements

Answer: D

Explanation:

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

QUESTION NO: 66

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

Answer: C
Explanation:

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

QUESTION NO: 67

The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

A.
generally accepted industry best practices.

B.
business requirements.

C.
legislative and regulatory requirements.

D.
storage availability.

Answer: B
Explanation:

The primary concern will be to comply with legislation and regulation but only if this is a genuine business requirement. Best practices may be a useful guide but not a primary concern. Legislative and regulatory requirements are only relevant if compliance is a business need. Storage is irrelevant since whatever is needed must be provided

QUESTION NO: 68

When personal information is transmitted across networks, there MUST be adequate controls over:

A.
change management.

B.
privacy protection.

C.
consent to data transfer.

D.
encryption devices.

Answer: B
Explanation:

Privacy protection is necessary to ensure that the receiving party has the appropriate level of protection of personal data. Change management primarily protects only the information, not the privacy of the individuals. Consent is one of the protections that is frequently, but not always, required. Encryption is a method of achieving the actual control, but controls over the devices may not ensure adequate privacy protection and, therefore, is a partial answer.

QUESTION NO: 69

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

A.
ensure that security processes are consistent across the organization.

B.
enforce baseline security levels across the organization.

C.
ensure that security processes are fully documented.

D.
implement monitoring of key performance indicators for security processes.

Answer: A
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 NO: 70

Who in an organization has the responsibility for classifying information?

A.
Data custodian

B.
Database administrator

C.
Information security officer

D.
Data owner

Answer: D
Explanation:

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

QUESTION NO: 71

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

A.
Defining and ratifying the classification structure of information assets

B.
Deciding the classification levels applied to the organization's information assets

C.
Securing information assets in accordance with their classification

D.
Checking if information assets have been classified properly

Answer: A
Explanation:

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

QUESTION NO: 72

Logging is an example of which type of defense against systems compromise?

A.
Containment

B.
Detection

C.
Reaction

D.
Recovery

Answer: B
Explanation:

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

QUESTION NO: 73

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

A.
Creating a positive business security environment

B.
Understanding key business objectives

C.
Having a reporting line to senior management

D.
Allocating sufficient resources to information security

Answer: B

Explanation:

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

QUESTION NO: 74

Who is ultimately responsible for the organization's information?

A.
Data custodian

B.
Chief information security officer (CISO)

C.
Board of directors

D.
Chief information officer (CIO)

Answer: C

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 NO: 75

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

A.
Alignment with industry best practices

B.
Business continuity investment

C.
Business benefits

D.
Regulatory compliance

Answer: D
Explanation:

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

QUESTION NO: 76

A security manager meeting the requirements for the international flow of personal data will need to ensure:

A.
a data processing agreement.

B.
a data protection registration.

C.
the agreement of the data subjects.

D.
subject access procedures.

Answer: C

Explanation:

Whenever personal data are transferred across national boundaries, the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

QUESTION NO: 77

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

A.
Ethics

B.
Proportionality

C.
Integration

D.
Accountability

Answer: B
Explanation:

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

QUESTION NO: 78

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

A.
Senior management commitment

B.
Information security framework

C.
Information security organizational structure

D.
Information security policy

Answer: A
Explanation:

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

QUESTION NO: 79

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

A.
Number of employees

B.
Distance between physical locations

C.
Complexity of organizational structure

D.
Organizational budget

Answer: C
Explanation:

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

QUESTION NO: 80

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

A.
prepare a security budget.

B.
conduct a risk assessment.

C.
develop an information security policy.

D.
obtain benchmarking information.

Answer: B
Explanation:

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

QUESTION NO: 81

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.

Answer: A
Explanation:

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

QUESTION NO: 82

An outcome of effective security governance is:

A.
business dependency assessment

B.
strategic alignment.

C.
risk assessment.

D.
planning.

Answer: B
Explanation:

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

QUESTION NO: 83

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

A.
Give organization standards preference over local regulations

B.
Follow local regulations only

C.
Make the organization aware of those standards where local regulations causes conflicts

D.
Negotiate a local version of the organization standards

Answer: D
Explanation:

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

QUESTION NO: 84

Who should drive the risk analysis for an organization?

A.
Senior management

B.
Security manager

C.
Quality manager

D.

Legal department

Answer: B

Explanation:

Although senior management should support and sponsor a risk analysis, the know-how and the management of the project will be with the security department. Quality management and the legal department will contribute to the project.

QUESTION NO: 85

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.

Answer: B

Explanation:

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

QUESTION NO: 86

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

Answer: A
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 NO: 87

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

A.
Risk assessment report

B.
Technical evaluation report

C.
Business case

D.
Budgetary requirements

Answer: C
Explanation:

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

QUESTION NO: 88

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

Answer: C
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 NO: 89

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

Answer: D
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 NO: 90

To achieve effective strategic alignment of security initiatives, it is important that:

A.
Steering committee leadership be selected by rotation.

B.
Inputs be obtained and consensus achieved between the major organizational units.

C.
The business strategy be updated periodically.

D.
Procedures and standards be approved by all departmental heads.

Answer: B
Explanation:

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

QUESTION NO: 91

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

A.
Man-in-the-middle attack

B.
Spoofing of data packets

C.
Rogue access point

D.
Session hijacking

Answer: C

Explanation:

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

QUESTION NO: 92

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

Answer: C

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 NO: 93

In implementing information security governance, the information security manager is PRIMARILY responsible for:

A.
developing the security strategy.

B.
reviewing the security strategy.

C.
communicating the security strategy.

D.
approving the security strategy

Answer: A

Explanation:

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

QUESTION NO: 94

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.

Answer: C
Explanation:

Strategic alignment of security with business objectives is a key indicator of performance measurement. In guiding a security program, a meaningful performance measurement will also rely on an understanding of business objectives, which will be an outcome of alignment. Business linkages do not by themselves indicate integration or value delivery. While alignment is an important precondition, it is not as important an indicator.

QUESTION NO: 95

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

A.
Compliance with international security standards.

B.
Use of a two-factor authentication system.

C.
Existence of an alternate hot site in case of business disruption.

D.
Compliance with the organization's information security requirements.

Answer: D
Explanation:

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

QUESTION NO: 96

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.

Answer: D

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 NO: 97

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

A.

attributes and characteristics of the 'desired state."

B.
overall control objectives of the security program.

C.
mapping the IT systems to key business processes.

D.
calculation of annual loss expectations.

Answer: A
Explanation:

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

QUESTION NO: 98

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

A.
develop a security architecture.

B.
install a network intrusion detection system (NIDS) and prepare a list of attacks.

C.
develop a network security policy.

D.
conduct a risk assessment.

Answer: D
Explanation:

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

QUESTION NO: 99

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

A.
Proficiency test

B.
Job descriptions

C.
Organization chart

D.
Skills inventory

Answer: D
Explanation:

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

QUESTION NO: 100

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

A.
state expectations of IT management.

B.

state only one general security mandate.

C.
are aligned with organizational goals.

D.
govern the creation of procedures and guidelines.

Answer: C
Explanation:

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

QUESTION NO: 101

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.

Answer: A
Explanation:

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

QUESTION NO: 102

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.

Answer: D
Explanation:

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

QUESTION NO: 103

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.

Answer: C
Explanation:

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

QUESTION NO: 104

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

Answer: A
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 NO: 105

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

Answer: A
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 NO: 106

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

Answer: C
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 NO: 107

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

A.
Cost reduction

B.
Compliance with company policies

C.
Protection of business assets

D.
Increased business value

Answer: D
Explanation:

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

QUESTION NO: 108

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.

Answer: A
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 NO: 109

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.

Answer: C

Explanation:

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

QUESTION NO: 110

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

A.
Key control monitoring

B.
A robust security awareness program

C.
A security program that enables business activities

D.
An effective security architecture

Answer: C

Explanation:

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

QUESTION NO: 111

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

A.
Continuous analysis, monitoring and feedback

B.
Continuous monitoring of the return on security investment (ROSD

C.
Continuous risk reduction

D.
Key risk indicator (KRD setup to security management processes

Answer: A
Explanation:

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

QUESTION NO: 112

The MOST complete business case for security solutions is one that.

A.
includes appropriate justification.

B.
explains the current risk profile.

C.
details regulatory requirements.

D.

identifies incidents and losses.

Answer: A

Explanation:

Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

QUESTION NO: 113

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

A.
Regulatory environment

B.
International security standards

C.
Organizational risks

D.
Organizational goals

Answer: D

Explanation:

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

QUESTION NO: 114

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.

Answer: B
Explanation:

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

QUESTION NO: 115

Which of the following would help to change an organization's security culture?

A.
Develop procedures to enforce the information security policy

B.
Obtain strong management support

C.
Implement strict technical security controls

D.
Periodically audit compliance with the information security policy

Answer: B
Explanation:

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

QUESTION NO: 116

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.

Answer: D
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 NO: 117

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

A.

conduct a risk assessment.

B.
conduct a workshop for all end users.

C.
prepare a security budget.

D.
obtain high-level sponsorship.

Answer: D
Explanation:

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

QUESTION NO: 118

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.

Answer: A
Explanation:

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

QUESTION NO: 119

An organization's information security strategy should be based on:

A.
managing risk relative to business objectives.

B.
managing risk to a zero level and minimizing insurance premiums.

C.
avoiding occurrence of risks so that insurance is not required.

D.
transferring most risks to insurers and saving on control costs.

Answer: A
Explanation:

Organizations must manage risks to a level that is acceptable for their business model, goals and objectives. A zero-level approach may be costly and not provide the effective benefit of additional revenue to the organization. Long-term maintenance of this approach may not be cost effective. Risks vary as business models, geography, and regulatory- and operational processes change. Insurance covers only a small portion of risks and requires that the organization have certain operational controls in place.

QUESTION NO: 120

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

A.
A cost-benefit analysis of budgeted resources

B.
All of the resources that are recommended by the business

C.
Total cost of ownership (TCO)

D.
Baseline comparisons

Answer: A
Explanation:

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

QUESTION NO: 121

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

Answer: A

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 NO: 122

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.

Answer: A

Explanation:

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

QUESTION NO: 123

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.

Answer: D
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 NO: 124

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).

Answer: A
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 NO: 125

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

A.
Laws and regulations of the country of origin may not be enforceable in the foreign country.

B.
A security breach notification might get delayed due to the time difference.

C.
Additional network intrusion detection sensors should be installed, resulting in an additional cost.

D.
The company could lose physical control over the server and be unable to monitor the physical security posture of the servers.

Answer: A
Explanation:

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

QUESTION NO: 126

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.

Answer: D
Explanation:

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

QUESTION NO: 127

The FIRST step to create an internal culture that focuses on information security is to:

A.
implement stronger controls.

B.
conduct periodic awareness training.

C.
actively monitor operations.

D.
gain the endorsement of executive management.

Answer: D
Explanation:

Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

QUESTION NO: 128

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.

Answer: A
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 NO: 129

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

A.
drafting information security policies.

B.
reviewing training and awareness programs.

C.

setting the strategic direction of the program.

D.
auditing for compliance.

Answer: C
Explanation:

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

QUESTION NO: 130

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

Answer: C
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 NO: 131

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

A.
The security officer

B.
Senior management

C.
The end user

D.
The custodian

Answer: B
Explanation:

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

QUESTION NO: 132

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

A.
Direct information security on what they need to do

B.
Research solutions to determine the proper solutions

C.
Require management to report on compliance

D.
Nothing; information security does not report to the board

Answer: C
Explanation:

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

QUESTION NO: 133

Information security should be:

A.
focused on eliminating all risks.

B.
a balance between technical and business requirements.

C.
driven by regulatory requirements.

D.
defined by the board of directors.

Answer: B
Explanation:

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

QUESTION NO: 134

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

A.
Realistic budget estimates

B.
Security awareness

C.
Support of senior management

D.
Recalculation of the work factor

Answer: C
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 NO: 135

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

Answer: D
Explanation:

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

QUESTION NO: 136

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

A.
the plan aligns with the organization's business plan.

B.
departmental budgets are allocated appropriately to pay for the plan.

C.
regulatory oversight requirements are met.

D.
the impact of the plan on the business units is reduced.

Answer: A
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 NO: 137

Which of the following should be determined while defining risk management strategies?

A.
Risk assessment criteria

B.
Organizational objectives and risk appetite

C.
IT architecture complexity

D.
Enterprise disaster recovery plans

Answer: B
Explanation:

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

QUESTION NO: 138

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

Answer: A
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.

QUESTION NO: 139

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

A.
To help determine the current state of risk

B.
To budget appropriately for needed controls

C.
To satisfy regulatory requirements

D.
To analyze the effect on the business

Answer: A
Explanation:

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

QUESTION NO: 140

Which of the following **BEST** enables the deployment of consistent security throughout international branches within a multinational organization?

A.
Maturity of security processes

B.
Remediation of audit findings

C.
Decentralization of security governance

D.
Establishment of security governance

Answer: D
Explanation:

QUESTION NO: 141

Which of the following is the **BEST** way to determine if an information security program aligns with corporate governance?

A.
Evaluate funding for security initiatives.

B.
Survey end users about corporate governance.

C.
Review information security policies.

D.
Review the balanced scorecard.

Answer: C
Explanation:
Explanation

One of the most important aspects of the action plan to execute the strategy is to create or modify, as needed, policies and standards. Policies are one of the primary elements of governance and each policy should state only one general security mandate. The road map should show the steps and the sequence, dependencies, and milestones.

QUESTION NO: 142

Security governance is **MOST** associated with which of the following IT infrastructure components?

A.
Network

B.
Application

C.
Platform

D.
Process

Answer: D
Explanation:

QUESTION NO: 143

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 would be in place.

B.
An effective security risk management process is established.

C.
End-user acceptance of emerging technologies has been established.

D.
A cost-benefit analysis process would be easier to perform.

Answer: B

Explanation:

QUESTION NO: 144

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.

Answer: A

Explanation:

QUESTION NO: 145

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

Answer: B

Explanation:

QUESTION NO: 146

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

Answer: A

Explanation:

QUESTION NO: 147

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.

Answer: A

Explanation:

QUESTION NO: 148

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.

Answer: D

Explanation:

QUESTION NO: 149

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.

Answer: C

Explanation:

QUESTION NO: 150

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.

Answer: B

Explanation:

QUESTION NO: 151

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.

Answer: A

Explanation:

QUESTION NO: 152

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

Answer: A

Explanation:

QUESTION NO: 153

Internal audit has reported a number of information security issues which are not in compliance with regulatory requirements. What should the information security manager do FIRST?

A.
Create a security exception

B.
Perform a vulnerability assessment

C.
Perform a gap analysis to determine needed resources

D.
Assess the risk to business operations

Answer: C

Explanation:

QUESTION NO: 154

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

Answer: B

Explanation:

QUESTION NO: 155

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.

Answer: A

Explanation:

QUESTION NO: 156

Which of the following is the **MOST** important consideration for designing an effective information security governance framework?

A.
Defined security metrics

B.
Continuous audit cycle

C.
Security policy provisions

D.
Security controls automation

Answer: A
Explanation:

QUESTION NO: 157

The **PRIMARY** goal of information security governance to an organization is to:

A.
align with business processes

B.
align with business objectives

C.
establish a security strategy

D.
manage security costs

Answer: B

Explanation:

QUESTION NO: 158

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.

Answer: C

Explanation:

QUESTION NO: 159

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

Answer: B

Explanation:

QUESTION NO: 160

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

Answer: B

Explanation:

QUESTION NO: 161

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

Answer: B

Explanation:

QUESTION NO: 162

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

Answer: C

Explanation:

QUESTION NO: 163

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.

Answer: B

Explanation:

QUESTION NO: 164

Which of the following is **MOST** helpful in integrating information security governance with corporate governance?

A.
Assigning the implementation of information security governance to the steering committee.

B.
Including information security processes within operational and management processes.

C.
Providing independent reports of information security efficiency and effectiveness to the board.

D.
Aligning the information security governance to a globally accepted framework.

Answer: B
Explanation:

QUESTION NO: 165

Which of the following is the **BEST** way to align security and business strategies?

A.
Include security risk as part of corporate risk management.

B.
Develop a balanced scorecard for security.

C.
Establish key performance indicators (KPIs) for business through security processes.

D.
Integrate information security governance into corporate governance.

Answer: C

Explanation:

QUESTION NO: 166

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.

Answer: B

Explanation:

QUESTION NO: 167

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.

Answer: A

Explanation:

QUESTION NO: 168

Which of the following would **BEST** help to ensure the alignment between information security and business functions?

A.
Developing information security polices

B.
Establishing an information security governance committee

C.
Establishing a security awareness program

D.
Providing funding for information security efforts

Answer: B
Explanation:

QUESTION NO: 169

When establishing an information security governance framework, it is **MOST** important for an information security manager to understand:

A.
the regulatory environment.

B.
information security best practices.

C.
the corporate culture.

D.
risk management techniques.

Answer: A

Explanation:

QUESTION NO: 170

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

Answer: A

Explanation:

QUESTION NO: 171

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

Answer: C

Explanation:

QUESTION NO: 172

A large organization is in the process of developing its information security program that involves working with several complex organizational functions. Which of the following will **BEST** enable the successful implementation of this program?

A.
Security governance

B.
Security policy

C.
Security metrics

D.
Security guidelines

Answer: A
Explanation:

QUESTION NO: 173

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

Answer: C

Explanation:

QUESTION NO: 174

An information security manager discovers that the organization’s new information security policy is not being followed across all departments. Which of the following should be of **GREATEST** concern to the information security manager?

A.
Different communication methods may be required for each business unit.

B.
Business unit management has not emphasized the importance of the new policy.

C.
The corresponding controls are viewed as prohibitive to business operations.

D.
The wording of the policy is not tailored to the audience.

Answer: C

Explanation:

QUESTION NO: 175

An organization has detected potential risk emerging from noncompliance with new regulations in its industry.

Which of the following is the **MOST** important reason to report this situation to senior management?

A.
The risk profile needs to be updated.

B.
An external review of the risk needs to be conducted.

C.

Specific monitoring controls need to be implemented.

D.
A benchmark analysis needs to be performed.

Answer: A
Explanation:

QUESTION NO: 176

Which of the following is the **BEST** way for an information security manager to identify compliance with information security policies within an organization?

A.
Analyze system logs.

B.
Conduct security awareness testing.

C.
Perform vulnerability assessments.

D.
Conduct periodic audits.

Answer: D
Explanation:

QUESTION NO: 177

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.

Answer: C
Explanation:

QUESTION NO: 178

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

Answer: B
Explanation:

QUESTION NO: 179

Which of the following is the **BEST** approach to identify noncompliance issues with legal, regulatory, and contractual requirements?

A.
Risk assessment

B.
Business impact analysis (BIA)

C.
Vulnerability assessment

D.

Gap analysis

Answer: D

Explanation:

QUESTION NO: 180

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.

Answer: D

Explanation:

QUESTION NO: 181

When an organization and its IT-hosting service provider are establishing a contract with each other, it is **MOST** important that the contract includes:

A.

details of expected security metrics.

B.

each party's security responsibilities.

C.

penalties for noncompliance with security policy.

D.
recovery time objectives (RTOs).

Answer: B
Explanation:

It's very important when organization start work with third party before signing the SLA negotiate the company current security needs and new security risk.

QUESTION NO: 182

Which of the following would be **MOST** useful to help senior management understand the status of information security compliance?

A.
Industry benchmarks

B.
Risk assessment results

C.
Business impact analysis (BIA) results

D.
Key performance indicators (KPIs)

Answer: D
Explanation:

QUESTION NO: 183

Which of the following is **MOST** likely to be included in an enterprise information security policy?

A.
Security monitoring strategy

B.
Audit trail review requirements

C.
Password composition requirements

D.
Consequences of noncompliance

Answer: D
Explanation:

QUESTION NO: 184

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.

Answer: D
Explanation:

QUESTION NO: 185

Which of the following should be the **PRIMARY** expectation of management when an organization introduces an information security governance framework?

A.
Optimized information security resources

B.
Consistent execution of information security strategy

C.
Improved accountability to shareholders

D.
Increased influence of security management

Answer: B
Explanation:

QUESTION NO: 186

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.

Answer: C
Explanation:

QUESTION NO: 187

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

Answer: C

Explanation:

QUESTION NO: 188

When making an outsourcing decision, which of the following functions is **MOST** important to retain within the organization?

A.

Security management

B.

Incident response

C.

Risk assessment

D.

Security governance

Answer: D

Explanation:

QUESTION NO: 189

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

Answer: C
Explanation:

QUESTION NO: 190

The **MOST** important outcome of information security governance is:

A.
business risk avoidance.

B.
informed decision making.

C.
alignment with business goals.

D.
alignment with compliance requirements.

Answer: C
Explanation:

QUESTION NO: 191

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.

Answer: D
Explanation:

QUESTION NO: 192

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

Answer: D
Explanation:

QUESTION NO: 193

Which of the following is MOST important to the successful implementation of an information security governance framework across the organization?

A.
Organizational security controls deployed in line with regulations

B.
Security management processes aligned with security objectives

C.

The existing organizational security culture

D.
Security policies that adhere to industry best practices

Answer: B
Explanation:

QUESTION NO: 194

Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?

A.
Align information security budget requests to organizational goals

B.
Ensure information security efforts support business goals

C.
Provide periodic IT balanced scorecards to senior management

D.
Ensure information security aligns with IT strategy

Answer: A
Explanation:

QUESTION NO: 195

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

Answer: D
Explanation:

QUESTION NO: 196

The **PRIMARY** purpose of implementing information security governance metrics is to:

A.
measure alignment with best practices.

B.
assess operational and program metrics.

C.
refine control operations,

D.
guide security towards the desired state.

Answer: D
Explanation:

QUESTION NO: 197

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

Answer: A
Explanation:

QUESTION NO: 198

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)

Answer: A
Explanation:

QUESTION NO: 199

Which of the following is the **BEST** approach for an information security manager to effectively manage third-party risk?

A.
Ensure controls are implemented to address changes in risk.

B.
Ensure senior management has approved the vendor relationship.

C.
Ensure risk management efforts are commensurate with risk exposure.

D.
Ensure vendor governance controls are in place.

Answer: D
Explanation:

QUESTION NO: 200

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.

Answer: B
Explanation:

QUESTION NO: 201

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.

Answer: A

Explanation:

QUESTION NO: 202

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

Answer: B

Explanation:

QUESTION NO: 203

When creating an information security governance program, which of the following will **BEST** enable the organization to address regulatory compliance requirements?

A.

Guidelines for processes and procedures

B.

A security control framework

C.

An approved security strategy plan

D.
Input from the security steering committee

Answer: A
Explanation:

QUESTION NO: 204

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

Answer: A
Explanation:

QUESTION NO: 205

Which of the following is the **BEST** evidence that an organization's information security governance framework is effective?

A.
Threats to the organization have diminished.

B.
The risk register is reviewed annually.

C.

The framework focuses primarily on technical controls.

D.
The framework can adapt to organizational changes.

Answer: A
Explanation:

QUESTION NO: 206

In information security governance, the **PRIMARY** role of the board of directors is to ensure:

A.
approval of relevant policies and standards.

B.
communication of security posture to stakeholders.

C.
compliance with regulations and best practices.

D.
alignment with the strategic goals of the organization.

Answer: D
Explanation:

QUESTION NO: 207

Which of the following is the **STRONGEST** indicator of effective alignment between corporate governance and information security governance?

A.
Senior management sponsors information security efforts.

B.
Senior management requests periodic information security updates.

C.
Key performance indicators (KPIs) for controls trend positively.

D.
Information security initiatives meet scope. schedule, and budget.

Answer: C
Explanation:

QUESTION NO: 208

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

Answer: A
Explanation:

QUESTION NO: 209

Who should decide the extent to which an organization will comply with new cybersecurity regulatory requirements?

A.
Senior management

B.
IT steering committee

C.
Legal counsel

D.
Information security manager

Answer: A
Explanation:

QUESTION NO: 210

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

Answer: D
Explanation:

QUESTION NO: 211

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

Answer: A
Explanation:

QUESTION NO: 212

Which of the following is the **BEST** option for addressing regulations that will adversely affect the allocation of information security program resources?

A.
Prioritize compliance efforts based on probability.

B.
Determine compliance levels of peer organizations.

C.
Delay implementation of compliance activities.

D.
Conduct assessments for management decisions

Answer: D
Explanation:

QUESTION NO: 213

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.

Answer: A
Explanation:

QUESTION NO: 214

Which of the following should be the **FIRST** step to ensure an information security program meets the requirements of new regulations?

A.
Validate the asset classification schema.

B.
Integrate compliance into the risk management process.

C.
Assess organizational security controls.

D.
Conduct a gap analysis to determine necessary changes.

Answer: B
Explanation:

QUESTION NO: 215

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 standards

D.
Local regulations

Answer: D
Explanation:

QUESTION NO: 216

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.

Answer: B
Explanation:

QUESTION NO: 217

During the establishment of a service level agreement (SLA) with a cloud service provider, it is **MOST** important for the information security manager to:

A.
update the security policy to reflect the provider's terms of service.

B.
ensure security requirements are contractually enforceable.

C.

set up proper communication paths with the provider.

D.
understand the cloud storage architecture in use to determine security risk.

Answer: B
Explanation:

QUESTION NO: 218

An outsourced vendor handles an organization's business-critical data.

Which of the following is the **MOST** effective way for the client organization to obtain assurance of the vendor's security practices?

A.
Verifying security certifications held by the vendor

B.
Reviewing the vendor's security audit reports

C.
Requiring periodic independent third-party reviews

D.
Requiring business continuity plans (BCPs) from the vendor

Answer: C
Explanation:

QUESTION NO: 219

Which of the following is **MOST** important when carrying out a forensic examination of a laptop to determine an employee's involvement in a fraud?

A.
The employee's network access should be suspended.

B.

The laptop should not be removed from the company premises.

C.
An HR representative should be present during the laptop examination.

D.
The investigation should be conducted on an image of the original disk drive.

Answer: D
Explanation:

QUESTION NO: 220

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

Answer: A
Explanation:

QUESTION NO: 221

Which of the following **BEST** demonstrates that the objectives of an information security governance framework are being met?

A.
Risk dashboard

B.
Key performance indicators (KPIs)

C.
Penetration test results

D.
Balanced scorecard

Answer: D
Explanation:

QUESTION NO: 222

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

Answer: C
Explanation:

QUESTION NO: 223

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

Answer: D
Explanation:

QUESTION NO: 224

The **PRIMARY** reason to classify information assets should be to ensure:

A.
proper access control.

B.
senior management buy-in.

C.
insurance valuation is appropriate.

D.
proper ownership is established.

Answer: D
Explanation:

Topic 2, INFORMATION RISK MANAGEMENT

QUESTION NO: 225

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

Answer: B
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 NO: 226

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

A.
Visibility and duration

B.
Likelihood and impact

C.
Probability and frequency

D.
Financial impact and duration

Answer: B
Explanation:

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

QUESTION NO: 227

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.

Answer: A
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 NO: 228

In assessing risk, it is MOST essential to:

A.
provide equal coverage for all asset types.

B.
use benchmarking data from similar organizations.

C.
consider both monetary value and likelihood of loss.

D.
focus primarily on threats and recent business losses.

Answer: C

Explanation:

A risk analysis should take into account the potential financial impact and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus primarily on recent losses or losses experienced by similar firms. Although this is important supplementary information, it does not reflect the organization's real situation. Geography and other factors come into play as well.

QUESTION NO: 229

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.

Answer: C
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 NO: 230

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

A.
Platform security

B.
Entitlement changes

C.
Intrusion detection

D.
Antivirus controls

Answer: B
Explanation:

Data owners are responsible for assigning user entitlements and approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

QUESTION NO: 231

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.

Answer: C
Explanation:

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

QUESTION NO: 232

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.

Answer: D
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 NO: 233

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.

Answer: D
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 NO: 234

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

A.
threat.

B.
loss.

C.
vulnerability.

D.
probability.

Answer: C
Explanation:

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

QUESTION NO: 235

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

A.
Evaluate productivity losses

B.
Assess the impact of confidential data disclosure

C.
Calculate the value of the information or asset

D.
Measure the probability of occurrence of each threat

Answer: C
Explanation:

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

QUESTION NO: 236

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.

Answer: A

Explanation:

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

QUESTION NO: 237

The valuation of IT assets should be performed by:

A.
an IT security manager.

B.
an independent security consultant.

C.
the chief financial officer (CFO).

D.
the information owner.

Answer: D

Explanation:

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

QUESTION NO: 238

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.

Answer: D

Explanation:

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

QUESTION NO: 239

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

A.
Senior management

B.
Business manager

C.
IT audit manager

D.
Information security officer (ISO)

Answer: B

Explanation:

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

QUESTION NO: 240

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.

Answer: C

Explanation:

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

QUESTION NO: 241

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.

Answer: B
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 NO: 242

Which of the following is MOST essential for a risk management program to be effective?

A.
Flexible security budget

B.
Sound risk baseline

C.
New risks detection

D.
Accurate risk reporting

Answer: C
Explanation:

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

QUESTION NO: 243

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

A.
Man-in-the-middle attack

B.
Brute force attack

C.
Remote buffer overflow

D.
Root kit

Answer: B
Explanation:

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

QUESTION NO: 244

Phishing is BEST mitigated by which of the following?

A.
Security monitoring software

B.
Encryption

C.
Two-factor authentication

D.
User awareness

Answer: D

Explanation:

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

QUESTION NO: 245

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.

Answer: D

Explanation:

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

QUESTION NO: 246

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

A.
business threats are constantly changing.

B.
omissions in earlier assessments can be addressed.

C.
repetitive assessments allow various methodologies.

D.
they help raise awareness on security in the business.

Answer: A
Explanation:

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

QUESTION NO: 247

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

A.
Identity business assets

B.
Identify business risks

C.
Assess vulnerabilities

D.
Evaluate key controls

Answer: A
Explanation:

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

QUESTION NO: 248

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.

Answer: A
Explanation:

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

QUESTION NO: 249

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

A.
Control

B.
Inherent

C.
Residual

D.
Audit

Answer: C
Explanation:

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

QUESTION NO: 250

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)

Answer: A
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 NO: 251

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.

Answer: B
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 NO: 252

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

A.
Programming

B.
Specification

C.

User testing

D.
Feasibility

Answer: D
Explanation:

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

QUESTION NO: 253

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

A.
Risk analysis process

B.
Business impact analysis (BIA)

C.
Risk management balanced scorecard

D.
Risk-based audit program

Answer: B
Explanation:

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

QUESTION NO: 254

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.

Answer: C
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 NO: 255

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

A.
Number of controls implemented

B.
Percent of control objectives accomplished

C.
Percent of compliance with the security policy

D.
Reduction in the number of reported security incidents

Answer: B
Explanation:

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

QUESTION NO: 256

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

A.
Strategic business plan

B.
Upcoming financial results

C.
Customer personal information

D.
Previous financial results

Answer: D
Explanation:

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

QUESTION NO: 257

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.

Answer: D
Explanation:

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

QUESTION NO: 258

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

Answer: C
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 NO: 259

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.

Answer: A
Explanation:

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

QUESTION NO: 260

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

A.
Business impact analyses

B.

Security gap analyses

C.
System performance metrics

D.
Incident response processes

Answer: B
Explanation:

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

QUESTION NO: 261

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.

Answer: D
Explanation:

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

QUESTION NO: 262

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

A.
Historical cost of the asset

B.
Acceptable level of potential business impacts

C.
Cost versus benefit of additional mitigating controls

D.
Annualized loss expectancy (ALE)

Answer: C
Explanation:

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

QUESTION NO: 263

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

A.
Understand the business requirements of the developer portal

B.
Perform a vulnerability assessment of the developer portal

C.
Install an intrusion detection system (IDS)

D.

Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Answer: A

Explanation:

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

QUESTION NO: 264

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

A.

Prevent the system from being accessed remotely

B.

Create a strong random password

C.

Ask for a vendor patch

D.

Track usage of the account by audit trails

Answer: B

Explanation:

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

QUESTION NO: 265

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

A.
a lack of proper input validation controls.

B.
weak authentication controls in the web application layer.

C.
flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.

D.
implicit web application trust relationships.

Answer: A
Explanation:

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

QUESTION NO: 266

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

A.
File backup procedures

B.
Database integrity checks

C.
Acceptable use policies

D.
Incident response procedures

Answer: C

Explanation:

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

QUESTION NO: 267

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

A.
Access control policy

B.
Data classification policy

C.
Encryption standards

D.
Acceptable use policy

Answer: B

Explanation:

Data classification policies define the level of protection to be provided for each category of data. Without this mandated ranking of degree of protection, it is difficult to determine what access controls or levels of encryption should be in place. An acceptable use policy is oriented more toward the end user and, therefore, would not specifically address what controls should be in place to adequately protect information.

QUESTION NO: 268

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

A.
Risk analysis

B.
Annualized loss expectancy (ALE) calculations

C.
Cost-benefit analysis

D.
Impact analysis

Answer: C
Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh 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 NO: 269

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)

Answer: C
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 NO: 270

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

Answer: A
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 NO: 271

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.

Answer: B
Explanation:

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

QUESTION NO: 272

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.

Answer: B
Explanation:

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

QUESTION NO: 273

The criticality and sensitivity of information assets is determined on the basis of:

A.
threat assessment.

B.
vulnerability assessment.

C.
resource dependency assessment.

D.
impact assessment.

Answer: D
Explanation:

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

QUESTION NO: 274

Which program element should be implemented FIRST in asset classification and control?

A.
Risk assessment

B.
Classification

C.
Valuation

D.
Risk mitigation

Answer: C
Explanation:

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

QUESTION NO: 275

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.

Answer: C
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 NO: 276

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.

Answer: C
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 NO: 277

The BEST strategy for risk management is to:

A.
achieve a balance between risk and organizational goals.

B.
reduce risk to an acceptable level.

C.
ensure that policy development properly considers organizational risks.

D.
ensure that all unmitigated risks are accepted by management.

Answer: B

Explanation:

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

QUESTION NO: 278

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

A.
Disclosure of personal information

B.
Sufficient coverage of the insurance policy for accidental losses

C.
Intrinsic value of the data stored on the equipment

D.
Replacement cost of the equipment

Answer: C
Explanation:

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

QUESTION NO: 279

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.

Answer: B
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 NO: 280

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

A.
Annual loss expectancy (ALE) of incidents

B.
Frequency of incidents

C.
Total cost of ownership (TCO)

D.
Approved budget for the project

Answer: C

Explanation:

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

QUESTION NO: 281

One way to determine control effectiveness is by determining:

A.
whether it is preventive, detective or compensatory.

B.
the capability of providing notification of failure.

C.
the test results of intended objectives.

D.
the evaluation and analysis of reliability.

Answer: C

Explanation:

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

QUESTION NO: 282

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

Answer: D
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 NO: 283

Who is responsible for ensuring that information is classified?

A.
Senior management

B.
Security manager

C.
Data owner

D.
Custodian

Answer: C
Explanation:

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

QUESTION NO: 284

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

A.
transferred.

B.
treated.

C.
accepted.

D.
terminated.

Answer: C

Explanation:

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

QUESTION NO: 285

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

Answer: B
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 NO: 286

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.

Answer: B
Explanation:

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

QUESTION NO: 287

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

Answer: D
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 NO: 288

To determine the selection of controls required to meet business objectives, an information security manager should:

A.
prioritize the use of role-based access controls.

B.
focus on key controls.

C.
restrict controls to only critical applications.

D.
focus on automated controls.

Answer: B

Explanation:

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

QUESTION NO: 289

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.

Answer: D

Explanation:

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

QUESTION NO: 290

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.

Answer: B
Explanation:

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

QUESTION NO: 291

Risk assessment is MOST effective when performed:

A.
at the beginning of security program development.

B.
on a continuous basis.

C.
while developing the business case for the security program.

D.
during the business change process.

Answer: B
Explanation:

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

QUESTION NO: 292

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

A.
Justification of the security budget must be continually made.

B.
New vulnerabilities are discovered every day.

C.
The risk environment is constantly changing.

D.
Management needs to be continually informed about emerging risks.

Answer: C
Explanation:

The risk environment is impacted by factors such as changes in technology, and business strategy. These changes introduce new threats and vulnerabilities to the organization. As a result, risk assessment should be performed continuously. Justification of a budget should never be the main reason for performing a risk assessment. New vulnerabilities should be managed through a patch management process. Informing management about emerging risks is important, but is not the main driver for determining when a risk assessment should be performed.

QUESTION NO: 293

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

A.
Identify the vulnerable systems and apply compensating controls

B.
Minimize the use of vulnerable systems

C.
Communicate the vulnerability to system users

D.

Update the signatures database of the intrusion detection system (IDS)

Answer: A

Explanation:

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

QUESTION NO: 294

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

A.

Business impact analysis (BIA)

B.

Penetration testing

C.

Audit and review

D.

Threat analysis

Answer: B

Explanation:

Penetration testing focuses on identifying vulnerabilities. None of the other choices would identify vulnerabilities introduced by changes.

QUESTION NO: 295

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

A.
Countermeasure cost-benefit analysis

B.
Penetration testing

C.
Frequent risk assessment programs

D.
Annual loss expectancy (ALE) calculation

Answer: A

Explanation:

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

QUESTION NO: 296

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.

Answer: C

Explanation:

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

QUESTION NO: 297

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

A.
Manager

B.
Custodian

C.
User

D.
Owner

Answer: D

Explanation:

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

QUESTION NO: 298

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.

Answer: B
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 NO: 299

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

A.
Key performance indicators (KPIs)

B.
Business impact analysis (BIA)

C.
Gap analysis

D.
Technical vulnerability assessment

Answer: C

Explanation:

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

QUESTION NO: 300

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

Answer: B

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 NO: 301

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

A.
User assessments of changes

B.
Comparison of the program results with industry standards

C.
Assignment of risk within the organization

D.
Participation by all members of the organization

Answer: D
Explanation:

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

QUESTION NO: 302

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.

Answer: C
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 NO: 303

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

A.
Define security metrics

B.
Conduct a risk assessment

C.
Perform a gap analysis

D.
Procure security tools

Answer: B
Explanation:

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

QUESTION NO: 304

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

A.
Downtime tolerance, resources and criticality

B.
Cost of business outages in a year as a factor of the security budget

C.
Business continuity testing methodology being deployed

D.
Structure of the crisis management team

Answer: A
Explanation:

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

QUESTION NO: 305

A risk management approach to information protection is:

A.
managing risks to an acceptable level, commensurate with goals and objectives.

B.
accepting the security posture provided by commercial security products.

C.
implementing a training program to educate individuals on information protection and risks.

D.
managing risk tools to ensure that they assess all information protection vulnerabilities.

Answer: A
Explanation:

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

QUESTION NO: 306

Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

A.
Implement countermeasures.

B.
Eliminate the risk.

C.
Transfer the risk.

D.
Accept the risk.

Answer: C
Explanation:

Risks are typically transferred to insurance companies when the probability of an incident is low but the impact is high. Examples include: hurricanes, tornados and earthquakes. Implementing countermeasures may not be the most cost-effective approach to security management. Eliminating the risk may not be possible. Accepting the risk would leave the organization vulnerable to a catastrophic disaster which may cripple or ruin the organization. It would be more cost effective to pay recurring insurance costs than to be affected by a disaster from which the organization cannot financially recover.

QUESTION NO: 307

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).

Answer: D
Explanation:

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

QUESTION NO: 308

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.

Answer: A
Explanation:

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

QUESTION NO: 309

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

A.
minimizing operational impacts.

B.
eliminating all vulnerabilities.

C.
usage by similar organizations.

D.
certification from a third party.

Answer: A
Explanation:

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

QUESTION NO: 310

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.

Answer: B

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 NO: 311

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)

Answer: C

Explanation:

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

QUESTION NO: 312

The purpose of a corrective control is to:

A.
reduce adverse events.

B.
indicate compromise.

C.
mitigate impact.

D.
ensure compliance.

Answer: C
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 NO: 313

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

Answer: D
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 NO: 314

Previously accepted risk should be:

A.
re-assessed periodically since the risk can be escalated to an unacceptable level due to revised conditions.

B.
accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptable.

C.
avoided next time since risk avoidance provides the best protection to the company.

D.
removed from the risk log once it is accepted.

Answer: A
Explanation:

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

QUESTION NO: 315

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

A.
perform a comprehensive assessment of the organization's exposure to the hacker's techniques.

B.
initiate awareness training to counter social engineering.

C.
immediately advise senior management of the elevated risk.

D.
increase monitoring activities to provide early detection of intrusion.

Answer: C
Explanation:

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

QUESTION NO: 316

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

A.
Staff interviews

B.
Threat identification

C.
Asset identification and valuation

D.
Determination of the likelihood of identified risks

Answer: C

Explanation:

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

QUESTION NO: 317

Which of the following authentication methods prevents authentication replay?

A.
Password hash implementation

B.
Challenge/response mechanism

C.
Wired Equivalent Privacy (WEP) encryption usage

D.
HTTP Basic Authentication

Answer: B

Explanation:

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

QUESTION NO: 318

An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

A.
Nothing, since a risk assessment was completed during development.

B.
A vulnerability assessment should be conducted.

C.
A new risk assessment should be performed.

D.
The new vendor's SAS 70 type II report should be reviewed.

Answer: C
Explanation:

The risk assessment process is continual and any changes to an established process should include a new- risk assessment. While a review of the SAS 70 report and a vulnerability assessment may be components of a risk assessment, neither would constitute sufficient due diligence on its own.

QUESTION NO: 319

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

A.
Senior management support

B.
Results of a cost-benefit analysis

C.
Results of a risk assessment

D.
Impact on the risk profile

Answer: D

Explanation:

Explanation

The information security manager must understand the business risk profile of the organization. No model provides a complete picture, but logically categorizing the risk areas of an organization facilitates focusing on key risk management strategies and decisions. It also enables the organization to develop and implement risk treatment approaches that are relevant to the business and cost effective.

QUESTION NO: 320

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.

Answer: A

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

QUESTION NO: 321

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.

Answer: B

Explanation:

QUESTION NO: 322

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 steering committees

Answer: B

Explanation:

QUESTION NO: 323

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.

Answer: B
Explanation:

QUESTION NO: 324

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

Answer: B
Explanation:

QUESTION NO: 325

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

A.

higher costs in supporting end users

B.
impact on network capacity

C.
decrease in end user productivity

D.
lack of a device management solution

Answer: D
Reference: https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

QUESTION NO: 326

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

Answer: C
Explanation:

QUESTION NO: 327

An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be MOST important to include when presenting the strategy to senior management?

A.
The costs associated with business process changes

B.
Results of benchmarking against industry peers

C.
The impact of organizational changes on the security risk profile

D.
Security controls needed for risk mitigation

Answer: C
Explanation:

QUESTION NO: 328

What is the BEST way to determine the level of risk associated with information assets processed by an IT application?

A.
Evaluate the potential value of information for an attacker

B.
Calculate the business value of the information assets

C.
Review the cost of acquiring the information assets for the business

D.
Research compliance requirements associated with the information

Answer: B
Explanation:

QUESTION NO: 329

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.

Answer: B
Explanation:

QUESTION NO: 330

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

Answer: A
Explanation:

QUESTION NO: 331

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.

Answer: C
Explanation:

QUESTION NO: 332

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.

Answer: A
Explanation:

QUESTION NO: 333

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

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

QUESTION NO: 334

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.

Answer: A
Explanation:

QUESTION NO: 335

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.

Answer: A
Explanation:

QUESTION NO: 336

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

Answer: B
Explanation:

QUESTION NO: 337

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

Answer: B
Explanation:

QUESTION NO: 338

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.

Answer: A
Explanation:

QUESTION NO: 339

When selecting risk response options to manage risk, an information security manager's **MAIN** focus should be on reducing:

A.

exposure to meet risk tolerance levels.

B.
the likelihood of threat.

C.
financial loss by transferring risk.

D.
the number of security vulnerabilities.

Answer: A
Explanation:

QUESTION NO: 340

Which of the following should an information security manager perform **FIRST** when an organization’s residual risk has increased?

A.
Implement security measures to reduce the risk.

B.
Communicate the information to senior management.

C.
Transfer the risk to third parties.

D.
Assess the business impact.

Answer: D
Explanation:

QUESTION NO: 341

Which of the following approaches is **BEST** for selecting controls to minimize information security risks?

A.

Cost-benefit analysis

B.
Control-effectiveness

C.
Risk assessment

D.
Industry best practices

Answer: C
Explanation:

QUESTION NO: 342

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

Answer: D
Explanation:

QUESTION NO: 343

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

Answer: A
Explanation:

QUESTION NO: 344

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.

Answer: A
Explanation:

QUESTION NO: 345

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.

Answer: D
Explanation:

QUESTION NO: 346

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

A.
Impact assessment

B.
Mitigation cost

C.
Threat assessment

D.
Vulnerability analysis

Answer: A
Explanation:

QUESTION NO: 347

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the **BEST** information to help maintain the security posture?

A.

Risk assessment

B.
Cloud security strategy

C.
Vulnerability assessment

D.
Risk governance framework

Answer: A
Explanation:

QUESTION NO: 348

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

Answer: A
Explanation:

QUESTION NO: 349

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

Answer: C

Explanation:

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 NO: 350

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.

Answer: A

Explanation:

QUESTION NO: 351

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

Answer: A
Explanation:

QUESTION NO: 352

Following a recent acquisition, an information security manager has been requested to address the outstanding risk reported early in the acquisition process. Which of the following would be the manager's **BEST** course of action?

A.
Add the outstanding risk to the acquiring organization's risk registry.

B.
Re-assess the outstanding risk of the acquired company.

C.
Re-evaluate the risk treatment plan for the outstanding risk.

D.
Perform a vulnerability assessment of the acquired company's infrastructure.

Answer: B
Explanation:

QUESTION NO: 353

An organization has recently experienced unauthorized device access to its network. To proactively manage the problem and mitigate this risk, the **BEST** preventive control would be to:

A.
keep an inventory of network and hardware addresses of all systems connected to the network.

B.
install a stateful inspection firewall to prevent unauthorized network traffic.

C.
implement network-level authentication and login to regulate access of devices to the network.

D.
deploy an automated asset inventory discovery tool to identify devices that access the network.

Answer: C
Explanation:

QUESTION NO: 354

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the **BEST** course of action to address the situation?

A.
Document the deficiencies in the risk register.

B.
Disconnect the legacy system from the rest of the network.

C.
Require that new systems that can meet the standards be implemented.

D.
Develop processes to compensate for the deficiencies.

Answer: A
Explanation:

QUESTION NO: 355

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.

Answer: B
Explanation:

QUESTION NO: 356

A risk management program will be **MOST** effective when:

A.
risk appetite is sustained for a long period

B.
risk assessments are repeated periodically

C.
risk assessments are conducted by a third party

D.
business units are involved in risk assessments

Answer: D
Explanation:

QUESTION NO: 357

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.

Answer: A
Explanation:

QUESTION NO: 358

The **MOST** important objective of monitoring key risk indicators (KRIs) related to information security is to:

A.
identify change in security exposures.

B.
reduce risk management costs.

C.
meet regulatory compliance requirements.

D.
minimize the loss from security incidents.

Answer: A
Explanation:

QUESTION NO: 359

Which of the following would be **MOST** helpful in determining an organization's current capacity to mitigate risk?

A.
Capability maturity model

B.
Business impact analysis

C.
IT security risk and exposure

D.
Vulnerability assessment

Answer: A
Explanation:

QUESTION NO: 360

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.

Answer: A
Explanation:

QUESTION NO: 361

An organization’s marketing department wants to use an online collaboration service which is not in compliance with the information security policy. A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

A.
the information security manager

B.
business senior management

C.
the chief risk officer

D.
the compliance officer.

Answer: D
Explanation:

QUESTION NO: 362

The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the **GREATEST** when:

A.
standard operating procedures are not formalized.

B.
the IT infrastructure is diverse.

C.
IDS sensors are misconfigured.

D.
operations and monitoring are handled by different teams.

Answer: A
Explanation:

QUESTION NO: 363

An information security manager has been informed of a new vulnerability in an online banking application, and patch to resolve this issue is expected to be released in the next 72 hours. The information security manager's **MOST** important course of action should be to:

A.
assess the risk and advise senior management.

B.
identify and implement mitigating controls.

C.
run the application system in offline mode.

D.
perform a business impact analysis (BIA).

Answer: A

Explanation:

QUESTION NO: 364

An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done **NEXT** to address this concern?

A.
Conduct a risk analysis

B.
Escalate to the chief risk officer

C.
Conduct a vulnerability analysis

D.
Determine compensating controls

Answer: A

Explanation:

QUESTION NO: 365

In risk assessment, after the identification of threats to organizational assets, the information security manager would:

A.
evaluate the controls currently in place.

B.
implement controls to achieve target risk levels.

C.
request funding for the security program.

D.
determine threats to be reported to upper management.

Answer: A
Explanation:

QUESTION NO: 366

During a security assessment, an information security manager finds a number of security patches were not installed on a server hosting a critical business application. The application owner did not approve the patch installation to avoid interrupting the application.

Which of the following should be the information security manager's **FIRST** course of action?

A.
Escalate the risk to senior management.

B.
Communicate the potential impact to the application owner.

C.
Report the risk to the information security steering committee.

D.
Determine mitigation options with IT management.

Answer: D
Explanation:

QUESTION NO: 367

Risk identification, analysis, and mitigation activities can **BEST** be integrated into business life cycle processes by linking them to:

A.
compliance testing

B.
configuration management

C.
continuity planning

D.
change management

Answer: B
Explanation:

QUESTION NO: 368

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.

Answer: C
Explanation:

QUESTION NO: 369

Which of the following would **BEST** justify spending for a compensating control?

A.
Threat analysis

B.
Risk analysis

C.
Peer benchmarking

D.
Vulnerability analysis

Answer: B
Explanation:

QUESTION NO: 370

After undertaking a security assessment of a production system, the information security manager is **MOST** likely to:

A.
inform the system owner of any residual risks and propose measures to reduce them.

B.
inform the development team of any residual risks, and together formulate risk reduction measures.

C.
inform the IT manager of the residual risks and propose measures to reduce them.

D.
establish an overall security program that minimizes the residual risks of that production system.

Answer: A
Explanation:

QUESTION NO: 371

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.

Answer: B
Explanation:

QUESTION NO: 372

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.

Answer: B
Explanation:

QUESTION NO: 373

Which of the following is the **MOST** important prerequisite to performing an information security risk assessment?

A.
Classifying assets

B.
Determining risk tolerance

C.
Reviewing the business impact analysis

D.
Assessing threats and vulnerabilities

Answer: D
Explanation:

QUESTION NO: 374

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.

Answer: D
Explanation:

QUESTION NO: 375

Reevaluation of risk is **MOST** critical when there is:

A.
a change in security policy.

B.
resistance to the implementation of mitigating controls.

C.
a change in the threat landscape.

D.
a management request for updated security reports.

Answer: C
Explanation:

QUESTION NO: 376

An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the **BEST** course of action for the information security manager?

A.
Present a business case for additional controls to senior management.

B.
Instruct IT to deploy controls based on urgent business needs.

C.
Solicit bids for compensating control products.

D.
Recommend a different application.

Answer: A
Explanation:

QUESTION NO: 377

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.

Answer: A

Explanation:

QUESTION NO: 378

Which of the following is the **MOST** important reason for performing a risk analysis?

A.
Assigning the appropriate level of protection

B.
Identifying critical information assets

C.
Identifying and eliminating threats

D.
Promoting increased security awareness in the organization

Answer: A

Explanation:

QUESTION NO: 379

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.

Answer: C
Explanation:

QUESTION NO: 380

A risk profile supports effective security decisions **PRIMARILY** because it:

A.
defines how to best mitigate future risks.

B.
identifies priorities for risk reduction.

C.
enables comparison with industry best practices.

D.
describes security threats.

Answer: B
Explanation:

QUESTION NO: 381

Which of the following would be the **MOST** effective to mitigate the risk of data loss in the event of a stolen laptop?

A.

Providing end-user awareness training focused on travelling with laptops

B.
Deploying end-point data loss prevention software on the laptop

C.
Encrypting the hard drive

D.
Utilizing a strong password

Answer: C

Explanation:

QUESTION NO: 382

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

Answer: A

Explanation:

QUESTION NO: 383

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

Answer: B

Explanation:

QUESTION NO: 384

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

Answer: C

Explanation:

QUESTION NO: 385

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

Answer: C

Explanation:

QUESTION NO: 386

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.

Answer: A

Explanation:

QUESTION NO: 387

Which of the following is the **MOST** effective mitigation strategy to protect confidential information from insider threats?

A.
Performing an entitlement review process

B.

Implementing authentication mechanisms

C.

Defining segregation of duties

D.

Establishing authorization controls

Answer: D

Explanation:

QUESTION NO: 388

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.

Answer: A

Explanation:

QUESTION NO: 389

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

Answer: A
Explanation:

QUESTION NO: 390

A risk mitigation report would include recommendations for:

A.
assessment.

B.
acceptance.

C.
evaluation.

D.
quantification.

Answer: B
Explanation:

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

QUESTION NO: 391

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.

Answer: B
Explanation:

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

QUESTION NO: 392

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

A.
risk assessments are not always precise.

B.
security risks are subject to frequent change.

C.
reviewers can optimize and reduce the cost of controls.

D.
it demonstrates to senior management that the security function can add value.

Answer: B
Explanation:

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

QUESTION NO: 393

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

A.
Overall risk is quantified

B.
Inherent risk is eliminated

C.
Residual risk is minimized

D.
Control risk is tied to business units

Answer: C
Explanation:

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

QUESTION NO: 394

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

A.
Theft of computer software

B.
Interruption of utility services

C.

Loss of customer confidence

D.
Internal fraud resulting in monetary loss

Answer: C
Explanation:

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

QUESTION NO: 395

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

A.
Risk analysis results

B.
Audit report findings

C.
Penetration test results

D.
Amount of IT budget available

Answer: A
Explanation:

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

QUESTION NO: 396

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

Answer: C
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 NO: 397

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.

Answer: D
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 NO: 398

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.

Answer: C

Explanation:

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

QUESTION NO: 399

Acceptable risk is achieved when:

A.
residual risk is minimized.

B.
transferred risk is minimized.

C.

control risk is minimized.

D.
inherent risk is minimized.

Answer: A
Explanation:

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

QUESTION NO: 400

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.

Answer: A
Explanation:

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

QUESTION NO: 401

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

Answer: A
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 NO: 402

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

A.
policy development.

B.
change management.

C.
awareness training.

D.
regular monitoring.

Answer: B

Explanation:

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

QUESTION NO: 403

Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

A.
Gap analysis

B.
Regression analysis

C.
Risk analysis

D.
Business impact analysis

Answer: D

Explanation:

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

QUESTION NO: 404

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

A.
Disaster declaration

B.
Recovery of the backups

C.
Restoration of the system

D.
Return to business as usual processing

Answer: C
Explanation:

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

QUESTION NO: 405

Which of the following results from the risk assessment process would BEST assist risk management decision making?

A.
Control risk

B.
Inherent risk

C.
Risk exposure

D.
Residual risk

Answer: D
Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

QUESTION NO: 406

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

Answer: B
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 NO: 407

Risk acceptance is a component of which of the following?

A.
Assessment

B.
Mitigation

C.
Evaluation

D.
Monitoring

Answer: B
Explanation:

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

QUESTION NO: 408

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.

Answer: C
Explanation:

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

QUESTION NO: 409

A risk assessment should be conducted:

A.
once a year for each business process and subprocess.

B.
every three to six months for critical business processes.

C.
by external parties to maintain objectivity.

D.
annually or whenever there is a significant change.

Answer: D
Explanation:

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

QUESTION NO: 410

The MOST important function of a risk management program is to:

A.
quantify overall risk.

B.
minimize residual risk.

C.
eliminate inherent risk.

D.
maximize the sum of all annualized loss expectancies (ALEs).

Answer: B

Explanation:

A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred; this is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

QUESTION NO: 411

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

A.
Theft of purchased software

B.
Power outage lasting 24 hours

C.
Permanent decline in customer confidence

D.
Temporary loss of e-mail due to a virus attack

Answer: C

Explanation:

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

QUESTION NO: 412

Which of the following will BEST prevent external security attacks?

A.
Static IP addressing

B.
Network address translation

C.
Background checks for temporary employees

D.
Securing and analyzing system access logs

Answer: B
Explanation:

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

QUESTION NO: 413

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.

Answer: D
Explanation:

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

QUESTION NO: 414

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.

Answer: B
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 NO: 415

When residual risk is minimized:

A.
acceptable risk is probable.

B.
transferred risk is acceptable.

C.
control risk is reduced.

D.
risk is transferable.

Answer: A
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 NO: 416

Quantitative risk analysis is MOST appropriate when assessment data:

A.
include customer perceptions.

B.
contain percentage estimates.

C.
do not contain specific details.

D.
contain subjective information.

Answer: B
Explanation:

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

QUESTION NO: 417

Which of the following is the MOST appropriate use of gap analysis?

A.
Evaluating a business impact analysis (BIA)

B.
Developing a balanced business scorecard

C.
Demonstrating the relationship between controls

D.
Measuring current state vs. desired future state

Answer: D
Explanation:

A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a business impact analysis (BIA), developing a balanced business scorecard or demonstrating the relationship between variables.

QUESTION NO: 418

Identification and prioritization of business risk enables project managers to:

A.
establish implementation milestones.

B.
reduce the overall amount of slack time.

C.
address areas with most significance.

D.
accelerate completion of critical paths.

Answer: C
Explanation:

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

QUESTION NO: 419

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.

Answer: C
Explanation:

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

QUESTION NO: 420

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

A.
Disaster declaration

B.
Before-image restoration

C.
System restoration

D.
After-image processing

Answer: B
Explanation:

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

QUESTION NO: 421

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

Answer: B
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 NO: 422

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

A.
Key financial systems

B.
Organizational activities

C.
Key systems and infrastructure

D.
Systems subject to regulatory compliance

Answer: B
Explanation:

Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

QUESTION NO: 423

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.

Answer: A

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 NO: 424

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

A.
Allows the organization to eliminate risk

B.
Is a necessary part of management's due diligence

C.
Satisfies audit and regulatory requirements

D.
Assists in incrementing the return on investment (ROD

Answer: B

Explanation:

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

QUESTION NO: 425

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

A.

External auditors

B.
A peer group within a similar business

C.
Process owners

D.
A specialized management consultant

Answer: C
Explanation:

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

QUESTION NO: 426

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.

Answer: A
Explanation:

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

QUESTION NO: 427

An information security manager has identified and implemented mitigating controls according to industry best practices. Which of the following is the **GREATEST** risk associated with this approach?

A.
The cost of control implementation may be too high.

B.
The security program may not be aligned with organizational objectives.

C.
The mitigation measures may not be updated in a timely manner.

D.
Important security controls may be missed without senior management input.

Answer: B
Explanation:

QUESTION NO: 428

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

Answer: B

Explanation:

QUESTION NO: 429

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.

Answer: B

Explanation:

QUESTION NO: 430

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

Answer: A

Explanation:

QUESTION NO: 431

Which of the following is the **MOST** effective method for categorizing system and data criticality during the risk assessment process?

A.
Interview senior management.

B.
Interview data custodians.

C.
Interview members of the board.

D.
Interview the asset owners.

Answer: D

Explanation:

QUESTION NO: 432

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

Answer: B

Explanation:

QUESTION NO: 433

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.

Answer: C

Explanation:

QUESTION NO: 434

Which of the following is the **MOST** important component of a risk profile?

A.
Risk management framework

B.
Data classification results

C.
Penetration test results

D.
Risk assessment methodology

Answer: A

Explanation:

QUESTION NO: 435

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

Answer: A

Explanation:

QUESTION NO: 436

Which of the following is **MOST** important for an information security manager to ensure is included in a business case for a new security system?

A.
Effectiveness of controls

B.
Risk reduction associated with the system

C.
Audit-logging capabilities

D.
Benchmarking results

Answer: B

Explanation:

QUESTION NO: 437

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.

Answer: D

Explanation:

QUESTION NO: 438

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.

Answer: D

Explanation:

QUESTION NO: 439

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.

Answer: C
Explanation:

QUESTION NO: 440

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

Answer: A

Explanation:

QUESTION NO: 441

Which of the following **BEST** promotes stakeholder accountability in the management of information security risks?

A.
Targeted security procedures

B.
Establishment of information ownership

C.
Establishment of security baselines

D.
Regular reviews for noncompliance

Answer: B

Explanation:

QUESTION NO: 442

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

Answer: D

Explanation:

QUESTION NO: 443

Application data integrity risk would be **MOST** directly addressed by a design that includes:

A.
access control technologies such as role-based entitlements.

B.
strict application of an authorized data dictionary.

C.
application log requirements such as field-level audit trails and user activity logs.

D.
reconciliation routines such as checksums, hash totals, and record counts.

Answer: D

Explanation:

QUESTION NO: 444

Which of the following is the **MOST** relevant risk factor to an organization when employees use social media?

A.
Social media can be accessed from multiple locations.

B.
Social media offers a platform that can host cyber-attacks.

C.
Social media can be used to gather intelligence for attacks.

D.
Social media increases the velocity of risk and the threat capacity.

Answer: C

Explanation:

QUESTION NO: 445

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.

Answer: B
Explanation:

QUESTION NO: 446

The **MOST** important reason to maintain key risk indicators (KRIs) is that:

A.
threats and vulnerabilities continuously evolve.

B.
they are needed to verify compliance with laws and regulations.

C.
they help assess the performance of the security program.

D.
management uses them to make informed business decisions.

Answer: A

Explanation:

QUESTION NO: 447

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

Answer: C
Explanation:

QUESTION NO: 448

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.

Answer: B

Explanation:

QUESTION NO: 449

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.

Answer: D
Explanation:

QUESTION NO: 450

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

Answer: B

Explanation:

QUESTION NO: 451

An information security manager is asked to provide a short presentation on the organization’s current IT risk posture to the board of directors. Which of the following would be **MOST** effective to include in this presentation?

A.
Risk heat map

B.
Gap analysis results

C.
Threat assessment results

D.
Risk register

Answer: A

Explanation:

QUESTION NO: 452

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.

Answer: A

Explanation:

QUESTION NO: 453

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.

Answer: A

Explanation:

QUESTION NO: 454

An organization is concerned with the risk of information leakage caused by incorrect use of personally owned smart devices by employees. What is the **BEST** way for the information security manager to mitigate the associated risk?

A.
Require employees to sign a nondisclosure agreement (NDA).

B.
Implement a mobile device management (MDM) solution.

C.
Document a bring-your-own-device (BYOD) policy.

D.
Implement a multi-factor authentication (MFA) solution.

Answer: B

Explanation:

QUESTION NO: 455

When determining an acceptable risk level, which of the following is the **MOST** important consideration?

A.
System criticalities

B.
Vulnerability scores

C.
Risk matrices

D.
Threat profiles

Answer: A

Explanation:

QUESTION NO: 456

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.

Answer: D

Explanation:

QUESTION NO: 457

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.

Answer: C

Explanation:

QUESTION NO: 458

An information security manager is evaluating the key risk indicators (KRIs) for an organization's information security program. Which of the following would be the information security manager's **GREATEST** concern?

A.
Undefined thresholds to trigger alerts

B.
Multiple KRIs for a single control process

C.
Use of qualitative measures

D.

Lack of formal KRI approval from IT management

Answer: A

Explanation:

QUESTION NO: 459

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

Answer: A

Explanation:

QUESTION NO: 460

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.

Answer: D

Explanation:

QUESTION NO: 461

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

Answer: B

Explanation:

QUESTION NO: 462

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)

Answer: C

Explanation:

QUESTION NO: 463

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

A.
Customer data stolen

B.
An electrical power outage

C.
A web site defaced by hackers

D.
Loss of the software development team

Answer: B
Explanation:

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

QUESTION NO: 464

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.

Answer: D
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 NO: 465

Which of the following is the MOST usable deliverable of an information security risk analysis?

A.
Business impact analysis (BIA) report

B.
List of action items to mitigate risk

C.
Assignment of risks to process owners

D.
Quantification of organizational risk

Answer: B
Explanation:

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

QUESTION NO: 466

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

A.
Tree diagrams

B.
Venn diagrams

C.
Heat charts

D.
Bar charts

Answer: C
Explanation:

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

QUESTION NO: 467

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

A.
business demands.

B.
inherent risks

C.
international standards.

D.
business risks.

Answer: D
Explanation:

QUESTION NO: 468

If the inherent risk of a business activity is higher than the acceptable risk level, the information security manager should **FIRST**:

A.
implement controls to mitigate the risk to an acceptable level.

B.
recommend that management avoids the business activity.

C.
assess the gap between current and acceptable level of risk.

D.
transfer risk to a third party to avoid cost of impact.

Answer: C
Explanation:

QUESTION NO: 469

Several identified risks have been mitigated to an acceptable level with appropriate controls. Which of the following activities would **BEST** help to maintain acceptable risk levels?

A.
Frequent assessments of inherent risks

B.
Periodic reviews of changes to the environment

C.
Periodic cost-benefit analyses of the implemented controls

D.
Frequent assessments of risk action plans

Answer: A
Explanation:

QUESTION NO: 470

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

Answer: A
Explanation:

QUESTION NO: 471

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.

Answer: B
Explanation:

QUESTION NO: 472

In order to understand an organization’s security posture, it is **MOST** important for an organization’s senior leadership to:

A.
ensure established security metrics are reported.

B.
review the number of reported security incidents.

C.
assess progress of risk mitigation efforts.

D.
evaluate results of the most recent incident response test.

Answer: A
Explanation:

QUESTION NO: 473

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)

Answer: D
Explanation:

QUESTION NO: 474

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

Answer: C
Explanation:

QUESTION NO: 475

When considering whether to adopt bring your own device (BYOD), it is **MOST** important for the information security manager to ensure that:

A.
business leaders have an understanding of security risks.

B.
users have read and signed acceptable use agreements.

C.
security controls are applied to each device when joining the network.

D.
the applications are tested prior to implementation.

Answer: A
Explanation:

QUESTION NO: 476

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

Answer: B
Explanation:

QUESTION NO: 477

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

Answer: C
Explanation:

QUESTION NO: 478

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.

Answer: D
Explanation:

QUESTION NO: 479

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.

Answer: D
Explanation:

QUESTION NO: 480

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

Answer: D
Explanation:

QUESTION NO: 481

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.

Answer: A
Explanation:

QUESTION NO: 482

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

Answer: D
Explanation:

Topic 3, INFORMATION SECURITY PROGRAM DEVELOPMENT

QUESTION NO: 483

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.

Answer: B
Explanation:

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

QUESTION NO: 484

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

A.
Redundant power supplies

B.
Protective switch covers

C.
Shutdown alarms

D.
Biometric readers

Answer: B
Explanation:

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

QUESTION NO: 485

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

A.
Tool for measuring effectiveness

B.
General understanding of goals

C.
Consistency with applicable standards

D.
Management sign-off and support initiatives

Answer: A
Explanation:

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

QUESTION NO: 486

What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A.
Authentication

B.
Encryption

C.
Prohibit employees from copying data to USB devices

D.
Limit the use of USB devices

Answer: B
Explanation:

Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

QUESTION NO: 487

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.

Answer: D
Explanation:

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

QUESTION NO: 488

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

A.
Strong authentication by password

B.
Encrypted hard drives

C.
Multifactor authentication procedures

D.

Network-based data backup

Answer: B

Explanation:

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

QUESTION NO: 489

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

A.
Reducing the human risk

B.
Maintaining evidence of training records to ensure compliance

C.
Informing business units about the security strategy

D.
Training personnel in security incident response

Answer: A

Explanation:

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

QUESTION NO: 490

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

A.
Requirements development

B.
Deployment

C.
Systems testing

D.
Code reviews

Answer: A

Explanation:

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

QUESTION NO: 491

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.

Answer: A

Explanation:

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

QUESTION NO: 492

Which of the following would be the BEST defense against sniffing?

A.
Password protect the files

B.
Implement a dynamic IP address scheme

C.
Encrypt the data being transmitted

D.
Set static mandatory access control (MAC) addresses

Answer: C

Explanation:

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

QUESTION NO: 493

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.

Answer: B
Explanation:

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

QUESTION NO: 494

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.

Answer: A

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 NO: 495

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

A.
Password-protected removable media

B.
Facsimile transmission in a secured room

C.
Using public key infrastructure (PKI) encryption

D.
Steganography

Answer: C

Explanation:

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

QUESTION NO: 496

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.

Answer: C

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 NO: 497

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

Answer: B

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 NO: 498

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.

Answer: C
Explanation:

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

QUESTION NO: 499

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

A.
Biometrics

B.
Symmetric encryption keys

C.
Secure Sockets Layer (SSL)-based authentication

D.
Two-factor authentication

Answer: D
Explanation:

Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

QUESTION NO: 500

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

Answer: D

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 NO: 501

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

A.
Filter media access control (MAC) addresses

B.
Use a Wi-Fi Protected Access (WPA2) protocol

C.
Use a Wired Equivalent Privacy (WEP) key

D.
Web-based authentication

Answer: B
Explanation:

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

QUESTION NO: 502

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

A.
An intrusion prevention system (IPS)

B.
An intrusion detection system (IDS)

C.
A host-based intrusion detection system (HIDS)

D.
A host-based firewall

Answer: A
Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect, but not prevent I IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

QUESTION NO: 503

Nonrepudiation can BEST be ensured by using:

A.
strong passwords.

B.
a digital hash.

C.
symmetric encryption.

D.
digital signatures.

Answer: D
Explanation:

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

QUESTION NO: 504

Which of the following tasks should be performed once a disaster recovery plan has been developed?

A.
Analyze the business impact.

B.
Define response team roles.

C.
Develop the test plan.

D.
Identify recovery time objectives.

Answer: B
Explanation:

QUESTION NO: 505

During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have **BEST** help to prevent this occurrence?

A.
Validation of senior management’s risk tolerance

B.
Updates to the business impact analysis (BIA)

C.
More effective disaster recovery plan (DRP) testing

D.

Improvements to incident identification methods

Answer: D

Explanation:

QUESTION NO: 506

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

Answer: D

Explanation:

QUESTION NO: 507

Which of the following defines the triggers within a business continuity plan (BCP)?

A.
Disaster recovery plan

B.
Needs of the organization

C.
Gap analysis

D.
Information security policy

Answer: A

Explanation:

QUESTION NO: 508

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

Answer: B

Explanation:

QUESTION NO: 509

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

Answer: C

Explanation:

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 NO: 510

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

Answer: C

Explanation:

QUESTION NO: 511

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the **MOST** useful information for planning purposes?

A.
Results from a gap analysis

B.

Results from a business impact analysis

C.
Deadlines and penalties for noncompliance

D.
An inventory of security controls currently in place

Answer: D
Explanation:

QUESTION NO: 512

A newly hired information security manager reviewing an existing security investment plan is **MOST** likely to be concerned when the plan:

A.
is based solely on a review of security threats and vulnerabilities in existing IT systems.

B.
identifies potential impacts that the implementation may have on business processes.

C.
focuses on compliance with common international security standards.

D.
has summarized IT costs for implementation rather than providing detail.

Answer: A
Explanation:

QUESTION NO: 513

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)

Answer: A
Explanation:

QUESTION NO: 514

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.

Answer: A
Explanation:

QUESTION NO: 515

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

Answer: A
Explanation:

QUESTION NO: 516

When developing an incident response plan, the information security manager should:

A.
include response scenarios that have been approved previously by business management.

B.
determine recovery time objectives (RTOs).

C.
allow IT to decide which systems can be removed from the infrastructure.

D.
require IT to invoke the business continuity plan.

Answer: B
Explanation:

QUESTION NO: 517

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.

Answer: D
Explanation:

QUESTION NO: 518

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between two offices. What should be the information security manager's **FIRST** course of action?

A.
Identify applicable regulatory requirements to establish security policies.

B.
Update privacy policies to include the other country's laws and regulations.

C.
Apply the current corporate security policies to the new office.

D.
Encrypt the data for transfer to the head office based on security manager approval.

Answer: A
Explanation:

QUESTION NO: 519

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain any effective information security program?

A.
Ensure information security is included in any change control efforts

B.
Merge the two information security programs to establish continuity

C.
Determine new factors that could influence the information security strategy

D.
Implement the current information security program in the acquired company

Answer: C
Explanation:

QUESTION NO: 520

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.

Answer: A
Explanation:

QUESTION NO: 521

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would **BEST** ensure that users adhere to the security standards?

A.
Monitor user activities on the network.

B.
Publish the standards on the intranet landing page.

C.
Establish an acceptable use policy.

D.
Deploy a device management solution.

Answer: D
Explanation:

QUESTION NO: 522

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)

Answer: C
Explanation:

QUESTION NO: 523

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

Answer: C

Explanation:

QUESTION NO: 524

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

Answer: D

Explanation:

QUESTION NO: 525

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.

Answer: B

Explanation:

QUESTION NO: 526

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

Answer: D

Explanation:

QUESTION NO: 527

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization’s information security strategy?

A.

Business impact analysis

B.
Organizational risk appetite

C.
Independent security audit

D.
Security risk assessment

Answer: A
Explanation:

QUESTION NO: 528

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

Answer: B
Explanation:

QUESTION NO: 529

Which of the following techniques would be the **BEST** test of security effectiveness?

A.
Performing an external penetration test

B.
Reviewing security policies and standards

C.
Reviewing security logs

D.
Analyzing technical security practices

Answer: B
Explanation:

QUESTION NO: 530

In the event that a password policy cannot be implemented for a legacy application, which of the following is the **BEST** course of action?

A.
Update the application security policy.

B.
Implement compensating control.

C.
Submit a waiver for the legacy application.

D.
Perform an application security assessment.

Answer: B
Explanation:

QUESTION NO: 531

To ensure the information security of outsourced IT services, which of the following is the **MOST** critical due diligence activity?

A.
Review samples of service level reports from the service provider.

B.
Assess the level of security awareness of the service provider.

C.
Request that the service provider comply with information security policy.

D.
Review the security status of the service provider.

Answer: C
Explanation:

QUESTION NO: 532

Management decisions concerning information security investments will be **MOST** effective when they are based on:

A.
an annual loss expectancy (ALE) determined from the history of security events.

B.
the formalized acceptance of risk analysis by management.

C.
the reporting of consistent and periodic assessments of risks.

D.
a process for identifying and analyzing threats and vulnerabilities.

Answer: C
Explanation:

QUESTION NO: 533

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.

Answer: D
Explanation:

QUESTION NO: 534

The **BEST** way to establish a recovery time objective (RTO) that balances cost with a realistic recovery time frame is to:

A.
perform a business impact analysis.

B.
determine daily downtime cost.

C.
analyze cost metrics.

D.
conduct a risk assessment.

Answer: A
Explanation:

QUESTION NO: 535

In a large organization, defining recovery time objectives (RTOs) is **PRIMARILY** the responsibility of:

A.
the IT manager.

B.
the information security manager.

C.
the business unit manager.

D.
senior manager.

Answer: D
Explanation:

QUESTION NO: 536

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

Answer: A
Explanation:

QUESTION NO: 537

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.

Answer: D
Explanation:

QUESTION NO: 538

Which of the following is the **PRIMARY** reason to conduct periodic business impact assessments?

A.
Improve the results of last business impact assessment

B.
Update recovery objectives based on new risks

C.
Decrease the recovery times

D.
Meet the needs of the business continuity policy

Answer: B
Explanation:

QUESTION NO: 539

Which of the following is the **BEST** approach to make strategic information security decisions?

A.
Establish an information security steering committee.

B.
Establish periodic senior management meetings.

C.
Establish regular information security status reporting.

D.
Establish business unit security working groups.

Answer: D

Explanation:

QUESTION NO: 540

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

Answer: A

Explanation:

QUESTION NO: 541

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.

Answer: B

Explanation:

QUESTION NO: 542

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

Answer: B

Explanation:

QUESTION NO: 543

An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personally identifiable information (PII).

Which of the following would be **MOST** helpful for this purpose?

A.
Metrics related to program effectiveness

B.
Written policies and standards

C.
Privacy awareness training

D.
Risk assessments of privacy-related applications

Answer: A
Explanation:

QUESTION NO: 544

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

Answer: A
Explanation:

QUESTION NO: 545

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

Answer: D
Explanation:

QUESTION NO: 546

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

Answer: A
Explanation:

QUESTION NO: 547

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

Answer: C
Explanation:

QUESTION NO: 548

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.

Answer: B
Explanation:

QUESTION NO: 549

Which of the following is the **MOST** important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

A.
The ability to remotely locate devices

B.
The ability to centrally manage devices

C.
The ability to restrict unapproved applications

D.
The ability to classify types of devices

Answer: B
Explanation:

QUESTION NO: 550

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

Answer: A
Explanation:

QUESTION NO: 551

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

Answer: C
Explanation:

QUESTION NO: 552

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.

Answer: C
Explanation:

QUESTION NO: 553

Which of the following is the **BEST** way to determine if an organization’s current risk is within the risk appetite?

A.

Conducting a business impact analysis (BIA)

B.
Implementing key performance indicators (KPIs)

C.
Implementing key risk indicators (KRIs)

D.
Developing additional mitigating controls

Answer: C
Explanation:

QUESTION NO: 554

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.

Answer: A
Explanation:

QUESTION NO: 555

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

Answer: C
Explanation:

QUESTION NO: 556

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.

Answer: A
Explanation:

QUESTION NO: 557

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.

Answer: A
Explanation:

QUESTION NO: 558

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.

Answer: A
Explanation:

QUESTION NO: 559

The chief information security officer (CISO) has developed an information security strategy, but is struggling to obtain senior management commitment for funds to implement the strategy.

Which of the following is the **MOST** likely reason?

A.
The strategy does not include a cost-benefit analysis.

B.
The CISO reports to the CIO.

C.
There was a lack of engagement with the business during development.

D.
The strategy does not comply with security standards.

Answer: A
Explanation:

QUESTION NO: 560

An organization wants to enable digital forensics for a business-critical application. Which of the following will **BEST** help to support this objective?

A.
Install biometric access control.

B.
Develop an incident response plan.

C.
Define data retention criteria.

D.
Enable activity logging.

Answer: D
Explanation:

QUESTION NO: 561

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

Answer: B
Explanation:

QUESTION NO: 562

Which of the following should be the **PRIMARY** goal of an information security manager when designing information security policies?

A.
Reducing organizational security risk

B.
Improving the protection of information

C.
Minimizing the cost of security controls

D.
Achieving organizational objectives

Answer: D

Explanation:

QUESTION NO: 563

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus **PRIMARILY** on defining:

A.
security metrics

B.
service level agreements (SLAs)

C.
risk-reporting methodologies

D.
security requirements for the process being outsourced

Answer: A
Explanation:

QUESTION NO: 564

When developing security processes for handling credit card data on the business unit’s information system, the information security manager should **FIRST**:

A.
review corporate policies regarding credit card information.

B.
implement the credit card companies’ security requirements.

C.
ensure that systems handle credit card data are segmented.

D.
review industry’s best practices for handling secure payments.

Answer: A

Explanation:

QUESTION NO: 565

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

Answer: A

Explanation:

QUESTION NO: 566

When developing an information security strategy, the **MOST** important requirement is that:

A.
standards capture the intent of management.

B.
a schedule is developed to achieve objectives.

C.
the desired outcome is known.

D.
critical success factors (CSFs) are developed.

Answer: A

Explanation:

QUESTION NO: 567

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.

Answer: D
Explanation:

QUESTION NO: 568

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

Answer: B

Explanation:

QUESTION NO: 569

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.

Answer: B

Explanation:

QUESTION NO: 570

Which of the following would be **MOST** helpful to the information security manager tasked with enforcing enhanced password standards?

A.
Conducting password strength testing

B.
Reeducating end users on creating strong complex passwords

C.
Implementing a centralized identity management system

D.

Implementing technical password controls to include strong complexity

Answer: C

Explanation:

QUESTION NO: 571

Which of the following is the **MOST** practical control that an organization can implement to prevent unauthorized downloading of data to universal serial bus (USB) storage devices?

A.
Two-factor authentication

B.
Restrict drive usage

C.
Strong encryption

D.
Disciplinary action

Answer: B

Explanation:

QUESTION NO: 572

Which of the following is the **BEST** method to determine whether an information security program meets an organization’s business objectives?

A.
Implement performance measures.

B.
Review against international security standards.

C.
Perform a business impact analysis (BIA).

D.

Conduct an annual enterprise-wide security evaluation.

Answer: A

Explanation:

QUESTION NO: 573

What is the **BEST** course of action when an information security manager finds an external service provider has not implemented adequate controls for safeguarding the organization’s critical data?

A.
Assess the impact of the control gap.

B.
Initiate contract renegotiations.

C.
Purchase additional insurance.

D.
Conduct a controls audit of the provider.

Answer: A

Explanation:

QUESTION NO: 574

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.

Answer: B

Explanation:

QUESTION NO: 575

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

Answer: C

Explanation:

QUESTION NO: 576

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).

Answer: A

Explanation:

QUESTION NO: 577

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

Answer: A

Explanation:

QUESTION NO: 578

The **PRIMARY** reason for establishing a data classification scheme is to identify:

A.
data ownership.

B.
data-retention strategy.

C.
appropriate controls.

D.
recovery priorities.

Answer: C

Explanation:

QUESTION NO: 579

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

Answer: C

Explanation:

QUESTION NO: 580

For an organization with operations in different parts of the world, the **BEST** approach for ensuring that security policies do not conflict with local laws and regulations is to:

A.
refer to an external global standard to avoid any regional conflict

B.
make policies at a sufficiently high level, so they are globally applicable

C.
adopt uniform policies

D.
establish a hierarchy of global and local policies

Answer: D

Explanation:

QUESTION NO: 581

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

Answer: A
Explanation:

QUESTION NO: 582

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.

Answer: C
Explanation:

QUESTION NO: 583

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

Answer: A
Explanation:

QUESTION NO: 584

Which of the following should be done **FIRST** when establishing security measures for personal data stored and processed on a human resources management system?

A.
Conduct a privacy impact assessment.

B.
Evaluate data encryption technologies.

C.
Move the system into a separate network.

D.
Conduct a vulnerability assessment.

Answer: A
Explanation:

QUESTION NO: 585

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

Answer: A
Explanation:

QUESTION NO: 586

Authorization can **BEST** be accomplished by establishing:

A.
the ownership of the data.

B.
what users can do when they are granted system access.

C.
whether users are who they say they are.

D.
how users identify themselves to information systems.

Answer: B
Explanation:

QUESTION NO: 587

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

Answer: C
Explanation:

QUESTION NO: 588

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.

Answer: B
Explanation:

QUESTION NO: 589

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.

Answer: B
Explanation:

QUESTION NO: 590

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

A.
Internal auditor

B.
Chief operating officer (COO)

C.
Steering committee

D.
IT management

Answer: C
Explanation:

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

QUESTION NO: 591

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

A.
Virtual private network (VPN)

B.
Firewalls and routers

C.
Biometric authentication

D.
Two-factor authentication

Answer: A
Explanation:

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

QUESTION NO: 592

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

A.
Packet filtering

B.
Intrusion detection

C.
Software upgrades

D.
Definition tables

Answer: D
Explanation:

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

QUESTION NO: 593

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

A.
Centralized

B.
Role-based

C.
Decentralized

D.
Discretionary

Answer: B
Explanation:

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

QUESTION NO: 594

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

A.
Router

B.
Firewall

C.
Mail relay

D.
Authentication server

Answer: C
Explanation:

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

QUESTION NO: 595

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.

Answer: C

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 NO: 596

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.

Answer: C

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 NO: 597

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.

Answer: C
Explanation:

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

QUESTION NO: 598

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

A.
password resets.

B.
reported incidents.

C.
incidents resolved.

D.
access rule violations.

Answer: B
Explanation:

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

QUESTION NO: 599

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.

Answer: A
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 NO: 600

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

Answer: C
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 NO: 601

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.

Answer: C
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 NO: 602

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.

Answer: B
Explanation:

QUESTION NO: 603

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.

Answer: C

Explanation:

QUESTION NO: 604

Which of the following would **BEST** enable an organization to effectively monitor the implementation of standardized configurations?

A.
Implement a separate change tracking system to record changes to configurations.

B.
Perform periodic audits to detect non-compliant configurations.

C.
Develop policies requiring use of the established benchmarks.

D.
Implement automated scanning against the established benchmarks.

Answer: D

Explanation:

QUESTION NO: 605

Which of the following should be the information security manager’s **NEXT** step following senior management approval of the information security strategy?

A.
Develop a security policy.

B.
Develop a budget.

C.
Perform a gap analysis.

D.

Form a steering committee.

Answer: A

Explanation:

QUESTION NO: 606

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

Answer: A

Explanation:

QUESTION NO: 607

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.

Answer: B

Explanation:

QUESTION NO: 608

Which of the following is the **PRIMARY** responsibility of the information security steering committee?

A.
Developing security polices aligned with the corporate and IT strategies

B.
Reviewing business cases where benefits have not been realized

C.
Identifying risks associated with new security initiatives

D.
Developing and presenting business cases for security initiatives

Answer: A

Explanation:

QUESTION NO: 609

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.

Answer: B

Explanation:

QUESTION NO: 610

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

Answer: B

Explanation:

QUESTION NO: 611

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

Answer: B

Explanation:

QUESTION NO: 612

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

Answer: B

Explanation:

QUESTION NO: 613

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

Answer: A

Explanation:

QUESTION NO: 614

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

Answer: D

Explanation:

QUESTION NO: 615

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

Answer: C

Explanation:

QUESTION NO: 616

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.

Answer: A

Explanation:

QUESTION NO: 617

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

Answer: B

Explanation:

QUESTION NO: 618

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

Answer: D

Explanation:

QUESTION NO: 619

Planning for the implementation of an information security program is MOST effective when it:

A.
uses decision trees to prioritize security projects

B.
applies gap analysis to current and future business plans

C.
uses risk-based analysis for security projects

D.
applies technology-driven solutions to identified needs

Answer: C

Explanation:

QUESTION NO: 620

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

Answer: D
Explanation:

QUESTION NO: 621

Management is questioning the need for several items in the information security budget proposal.

Which of the following would have been **MOST** helpful prior to budget submission?

A.
Benchmarking information security efforts of industry competitors

B.
Obtaining better pricing from information security service vendors

C.
Presenting a report of current threats to the organization

D.
Educating management on information security best practices

Answer: C

Explanation:

QUESTION NO: 622

For a business operating in a competitive and evolving online market, it is **MOST** important for a security policy to focus on:

A.
defining policies for new technologies.

B.
enabling adoption of new technologies.

C.
requiring accreditation for new technologies.

D.
managing risks of new technologies.

Answer: D

Explanation:

QUESTION NO: 623

The **FIRST** step in establishing an information security program is to:

A.
define policies and standards that mitigate the organization’s risks.

B.
secure organizational commitment and support.

C.
assess the organization’s compliance with regulatory requirements.

D.
determine the level of risk that is acceptable to senior management.

Answer: B

Explanation:

QUESTION NO: 624

Which of the following would be **MOST** important to include in a business case to help obtain senior management’s commitment for an information security investment?

A.
Results of an independent audit

B.
Industry best practices

C.
Projected business value

D.
Reference to business polices

Answer: C
Explanation:

QUESTION NO: 625

In an organization with effective IT risk management, the **PRIMARY** reason to establish key risk indicators (KRIs) is to:

A.
provide information to remediate risk events.

B.
demonstrate the alignment of risk management efforts.

C.
map potential risk to key organizational strategic initiatives.

D.
identity triggers that exceed risk thresholds.

Answer: C

Explanation:

QUESTION NO: 626

Which of the following is the BEST way for an information security manager to justify continued investment in the information security program when the organization is facing significant budget cuts?

A.
Demonstrate that the program enables business activities

B.
Demonstrate an increase in ransomware attacks targeting peer organizations

C.
Demonstrate that implemented program controls are effective

D.
Demonstrate the readiness of business continuity plans

Answer: A

Explanation:

QUESTION NO: 627

Which of the following is the MOST important consideration when designing information security architecture?

A.
Risk management parameters for the organization are defined.

B.
The information security architecture is aligned with industry standards.

C.
The level of security supported is based on business decisions.

D.
The existing threat landscape is monitored.

Answer: C

Explanation:

QUESTION NO: 628

Which of the following processes if the FIRST step in establishing an information security policy?

A.
Security controls evaluation

B.
Information security audit

C.
Review of current global standards

D.
Business risk assessment

Answer: D

Explanation:

QUESTION NO: 629

A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?

A.
The organizations have different risk appetites

B.
Differing security technologies

C.
Differing security skills within the organizations

D.
Confidential information could be leaked

Answer: A

Explanation:

QUESTION NO: 630

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

Answer: C

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 NO: 631

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

A.
Patch management

B.
Change management

C.
Security baselines

D.
Virus detection

Answer: B
Explanation:

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

QUESTION NO: 632

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

A.
Gantt chart

B.
Waterfall chart

C.
Critical path

D.
Rapid Application Development (RAD)

Answer: C
Explanation:

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

QUESTION NO: 633

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

A.
Patch management

B.
Change management

C.
Security baselines

D.
Configuration management

Answer: A
Explanation:

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

QUESTION NO: 634

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.

Answer: D

Explanation:

QUESTION NO: 635

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

Answer: C

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 NO: 636

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

A.
Baseline security standards

B.
System access violation logs

C.
Role-based access controls

D.
Exit routines

Answer: C
Explanation:

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

QUESTION NO: 637

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

A.
Biometric authentication

B.
Embedded steganographic

C.
Two-factor authentication

D.
Embedded digital signature

Answer: D
Explanation:

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

QUESTION NO: 638

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A.
Daily

B.
Weekly

C.
Concurrently with O/S patch updates

D.
During scheduled change control updates

Answer: A

Explanation:

New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.

QUESTION NO: 639

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

A.
Network switch

B.
Web server

C.
Database server

D.

File/print server

Answer: B

Explanation:

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

QUESTION NO: 640

On which of the following should a firewall be placed?

A.
Web server

B.
Intrusion detection system (IDS) server

C.
Screened subnet

D.
Domain boundary

Answer: D

Explanation:

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

QUESTION NO: 641

An intranet server should generally be placed on the:

A.
internal network.

B.
firewall server.

C.
external router.

D.
primary domain controller.

Answer: A

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 NO: 642

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

A.
data encryption.

B.
digital signatures.

C.
strong passwords.

D.
two-factor authentication.

Answer: D

Explanation:

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

QUESTION NO: 643

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

A.
Centralizing security management

B.
Implementing sanctions for noncompliance

C.
Policy enforcement by IT management

D.
Periodic compliance reviews

Answer: A
Explanation:

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

QUESTION NO: 644

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

A.
Decrease in intrusion incidents

B.
Increase in reported incidents

C.
Decrease in security policy changes

D.
Increase in access rule violations

Answer: B
Explanation:

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

QUESTION NO: 645

The information classification scheme should:

A.
consider possible impact of a security breach.

B.
classify personal information in electronic form.

C.
be performed by the information security manager.

D.
classify systems according to the data processed.

Answer: A
Explanation:

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager.

QUESTION NO: 646

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

A.
Interoffice a system-generated complex password with 30 days expiration

B.
Give a dummy password over the telephone set for immediate expiration

C.
Require no password but force the user to set their own in 10 days

D.
Set initial password equal to the user ID with expiration in 30 days

Answer: B
Explanation:

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

QUESTION NO: 647

An information security program should be sponsored by:

A.
infrastructure management.

B.
the corporate audit department.

C.
key business process owners.

D.
information security management.

Answer: C
Explanation:

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

QUESTION NO: 648

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

A.
Termination conditions

B.
Liability limits

C.
Service levels

D.
Privacy restrictions

Answer: C

Explanation:

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

QUESTION NO: 649

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

A.
number of attacks blocked.

B.
number of packets dropped.

C.
average throughput rate.

D.
number of firewall rules.

Answer: A
Explanation:

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

QUESTION NO: 650

Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

A.
Patch management

B.

Change management

C.
Security baselines

D.
Acquisition management

Answer: A
Explanation:

Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Acquisition management controls the purchasing process.

QUESTION NO: 651

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.

Answer: A
Explanation:

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

QUESTION NO: 652

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

A.
SWOT analysis

B.
Waterfall chart

C.
Gap analysis

D.
Balanced scorecard

Answer: D
Explanation:

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

QUESTION NO: 653

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

A.
Patch management

B.
Change management

C.
Security metrics

D.
Version control

Answer: B

Explanation:

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

QUESTION NO: 654

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

Answer: B

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 NO: 655

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

A.
Security' awareness training

B.
Achievable goals and objectives

C.
Senior management sponsorship

D.
Adequate start-up budget and staffing

Answer: C

Explanation:

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

QUESTION NO: 656

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

A.
Adequate training on emerging security technologies

B.
Open communication with key process owners

C.
Adequate policies, standards and procedures

D.
Executive management commitment

Answer: D

Explanation:

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

QUESTION NO: 657

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

A.
Screened subnets

B.
Information classification policies and procedures

C.
Role-based access controls

D.
Intrusion detection system (IDS)

Answer: A
Explanation:

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

QUESTION NO: 658

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

A.
Intrusion detection system (IDS)

B.
IP address packet filtering

C.
Two-factor authentication

D.
Embedded digital signature

Answer: C
Explanation:

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

QUESTION NO: 659

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

Answer: D

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 NO: 660

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

A.
Proxy server

B.
Application server

C.
Departmental server

D.
Data warehouse server

Answer: B
Explanation:

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

QUESTION NO: 661

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

A.
Web server

B.
IDS server

C.
Screened subnet

D.
Domain boundary

Answer: D
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 NO: 662

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

A.
Internal network

B.
Demilitarized zone (DMZ)

C.
Database server

D.
Domain controller

Answer: B
Explanation:

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

QUESTION NO: 663

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.

Answer: A
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 NO: 664

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

Answer: D

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 NO: 665

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

A.
Tuning

B.
Patching

C.
Encryption

D.
Packet filtering

Answer: A

Explanation:

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

QUESTION NO: 666

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

A.
Authentication

B.
Hardening

C.
Encryption

D.
Nonrepudiation

Answer: C
Explanation:

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

QUESTION NO: 667

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

A.
Log all account usage and send it to their manager

B.
Establish predetermined automatic expiration dates

C.
Require managers to e-mail security when the user leaves

D.
Ensure each individual has signed a security acknowledgement

Answer: B

Explanation:

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

QUESTION NO: 668

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.

Answer: C
Explanation:

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

QUESTION NO: 669

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

A.

Ease of installation

B.
Product documentation

C.
Available support

D.
System overhead

Answer: D
Explanation:

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

QUESTION NO: 670

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

A.
Never use open source tools

B.
Focus only on production servers

C.
Follow a linear process for attacks

D.
Do not interrupt production processes

Answer: D
Explanation:

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

QUESTION NO: 671

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

Answer: C
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 NO: 672

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

A.
helps ensure that communications are secure.

B.
increases security between multi-tier systems.

C.
allows passwords to be changed less frequently.

D.
eliminates the need for secondary authentication.

Answer: A
Explanation:

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

QUESTION NO: 673

Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

A.
Boundary router

B.
Strong encryption

C.
Internet-facing firewall

D.
Intrusion detection system (IDS)

Answer: B
Explanation:

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

QUESTION NO: 674

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

A.
Firewall blocking rules

B.
Up-to-date signature files

C.
Security awareness training

D.
Intrusion detection monitoring

Answer: C

Explanation:

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

QUESTION NO: 675

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

A.
The firewall should block all inbound traffic during the outage

B.
All systems should block new logins until the problem is corrected

C.
Access control should fall back to no synchronized mode

D.
System logs should record all user activity for later analysis

Answer: C

Explanation:

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

QUESTION NO: 676

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

Answer: C
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 NO: 677

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

Answer: A
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 NO: 678

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

A.
Configuration of firewalls

B.
Strength of encryption algorithms

C.
Authentication within application

D.
Safeguards over keys

Answer: D
Explanation:

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

QUESTION NO: 679

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

A.
Encryption

B.
Digital certificate

C.
Digital signature

D.
I lashing algorithm

Answer: A

Explanation:

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

QUESTION NO: 680

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

A.
create more overhead than signature-based IDSs.

B.
cause false positives from minor changes to system variables.

C.
generate false alarms from varying user or system actions.

D.
cannot detect new types of attacks.

Answer: C
Explanation:

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

QUESTION NO: 681

An information security manager uses security metrics to measure the:

A.
performance of the information security program.

B.
performance of the security baseline.

C.
effectiveness of the security risk analysis.

D.
effectiveness of the incident response team.

Answer: A

Explanation:

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

QUESTION NO: 682

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

A.
customize the content to the target audience.

B.
ensure senior management is represented.

C.
ensure that all the staff is trained.

D.
avoid technical content but give concrete examples.

Answer: A

Explanation:

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

QUESTION NO: 683

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

Answer: B
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 NO: 684

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

A.
Certificate-based authentication of web client

B.
Certificate-based authentication of web server

C.
Data confidentiality between client and web server

D.
Multiple encryption algorithms

Answer: A

Explanation:

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

QUESTION NO: 685

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).

Answer: A

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 NO: 686

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.

Answer: C
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 NO: 687

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

A.
IP spoofing

B.
Man-in-the-middle attack

C.
Repudiation

D.
Trojan

Answer: D

Explanation:

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

QUESTION NO: 688

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

A.
Security compliant servers trend report

B.
Percentage of security compliant servers

C.
Number of security patches applied

D.
Security patches applied trend report

Answer: A

Explanation:

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

QUESTION NO: 689

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

A.
critical information resources needing protection.

B.
a security policy for the entire organization.

C.
the minimum acceptable security to be implemented.

D.
required physical and logical access controls.

Answer: C
Explanation:

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

QUESTION NO: 690

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

A.
Symmetric cryptography

B.
Public key infrastructure (PKI)

C.
Message hashing

D.
Message authentication code

Answer: B

Explanation:

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

QUESTION NO: 691

When creating an incident response plan, the **PRIMARY** benefit of establishing a clear definition of a security incident is that it helps to:

A.
communicate the incident response process to stakeholders

B.
develop effective escalation and response procedures

C.
make tabletop testing more effective

D.
adequately staff and train incident response teams

Answer: B
Explanation:

QUESTION NO: 692

Which of the following is the information security manager's PRIMARY role in the information assets classification process?

A.
Assigning asset ownership

B.

Assigning the asset classification level

C.
Securing assets in accordance with their classification

D.
Developing an asset classification model

Answer: D

Explanation:

QUESTION NO: 693

An organization plans to leverage popular social network platforms to promote its products and services. Which of the following is the **BEST** course of action for the information security manager to support this initiative?

A.
Develop security controls for the use of social networks

B.
Assess the security risk associated with the use of social networks

C.
Establish processes to publish content on social networks

D.
Conduct vulnerability assessments on social network platforms

Answer: C

Explanation:

QUESTION NO: 694

A multinational organization has developed a bring your own device (BYOD) policy that requires the installation of mobile device management (MDM) software on personally owned devices. Which of the following poses the **GREATEST** challenge for implementing the police?

A.

Varying employee data privacy rights

B.
Translation and communication of policy

C.
Differences in mobile OS platforms

D.
Differences in corporate cultures

Answer: C
Explanation:

QUESTION NO: 695

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

Answer: D
Explanation:

QUESTION NO: 696

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.

Answer: B
Explanation:

QUESTION NO: 697

An information security manager is developing a new information security strategy.

Which of the following functions would serve as the **BEST** resource to review the strategy and provide guidance for business alignment?

A.
Internal audit

B.
The steering committee

C.
The legal department

D.
The board of directors

Answer: B
Explanation:

QUESTION NO: 698

When integrating information security requirements into software development, which of the following practices should be **FIRST** in the development lifecycle?

A.
Penetration testing

B.
Dynamic code analysis

C.
Threat modeling

D.
Source code review

Answer: C
Explanation:

QUESTION NO: 699

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

Answer: D
Explanation:

QUESTION NO: 700

When developing a protection strategy for outsourcing applications, the information security manager **MUST** ensure that:

A.
escrow agreements are in place.

B.
the security requirements are included in the service level agreement (SLA).

C.
the responsibility for security is transferred in the service level agreement (SLA).

D.
nondisclosure clauses are in the contract.

Answer: B

Explanation:

QUESTION NO: 701

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

Answer: C

Explanation:

QUESTION NO: 702

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.

Answer: B
Explanation:

QUESTION NO: 703

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

Answer: A
Explanation:

QUESTION NO: 704

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.

Answer: A
Explanation:

QUESTION NO: 705

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.

Answer: D
Explanation:

QUESTION NO: 706

When evaluating vendors for sensitive data processing, which of the following should be the **FIRST** step to ensure the correct level of information security is provided?

A.
Include information security clauses in the vendor contract.

B.
Review third-party reports of potential vendors.

C.
Include information security criteria as part of vendor selection.

D.
Develop metrics for vendor performance.

Answer: C
Explanation:

QUESTION NO: 707

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:

Answer: A
Explanation:

QUESTION NO: 708

Which of the following is the **MOST** effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?

A.
Auditing the service delivery of third-party providers

B.
Including information security clauses within contracts

C.
Providing information security training to third-party personnel

D.
Requiring third parties to sign confidentiality agreements

Answer: B
Explanation:

QUESTION NO: 709

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

Answer: B
Explanation:

QUESTION NO: 710

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

Answer: B
Explanation:

QUESTION NO: 711

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

Answer: A
Explanation:

QUESTION NO: 712

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

Answer: A
Explanation:

QUESTION NO: 713

Which of the following security characteristics is **MOST** important to the protection of customer data in an online transaction system?

A.
Availability

B.
Data segregation

C.
Audit monitoring

D.
Authentication

Answer: D
Explanation:

QUESTION NO: 714

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

Answer: C
Explanation:

QUESTION NO: 715

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.

Answer: B
Explanation:

QUESTION NO: 716

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.

Answer: C

Explanation:

QUESTION NO: 717

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

Answer: A

Explanation:

QUESTION NO: 718

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

Answer: B

Explanation:

QUESTION NO: 719

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

Answer: D

Explanation:

QUESTION NO: 720

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)

Answer: D
Explanation:

QUESTION NO: 721

The **PRIMARY** reason for classifying assets is to:

A.
balance asset value and protection measures.

B.
identify low-value assets with insufficient controls.

C.
establish clear lines of authority and ownership for the asset.

D.
inform senior management of the organization's risk posture.

Answer: A
Explanation:

QUESTION NO: 722

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.

Answer: A
Explanation:

QUESTION NO: 723

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.

Answer: C
Explanation:

QUESTION NO: 724

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.

Answer: B
Explanation:

QUESTION NO: 725

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

Answer: A
Explanation:

QUESTION NO: 726

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.

Answer: B
Explanation:

QUESTION NO: 727

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

Answer: A
Explanation:

QUESTION NO: 728

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

Answer: C
Explanation:

QUESTION NO: 729

Which of the following **BEST** determines an information asset's classification?

A.
Directives from the data owner

B.
Criticality to a business process

C.
Cost of producing the information asset

D.
Value of the information asset to competitors

Answer: B
Explanation:

QUESTION NO: 730

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

Answer: A
Explanation:

QUESTION NO: 731

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

A.
Regular review of access control lists

B.
Security guard escort of visitors

C.
Visitor registry log at the door

D.
A biometric coupled with a PIN

Answer: A
Explanation:

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

QUESTION NO: 732

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A.
revise the information security program.

B.
evaluate a balanced business scorecard.

C.
conduct regular user awareness sessions.

D.
perform penetration tests.

Answer: B
Explanation:

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

QUESTION NO: 733

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

A.
The definition of roles and responsibilities

B.
The scope of the security program

C.
The key objectives of the security program

D.
Reference to procedures and standards of the security program

Answer: C

Explanation:

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

QUESTION NO: 734

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.

Answer: A

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 NO: 735

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.

Answer: D
Explanation:

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

QUESTION NO: 736

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

A.
Number of controls

B.
Cost of achieving control objectives

C.
Effectiveness of controls

D.
Test results of controls

Answer: B
Explanation:

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

QUESTION NO: 737

Which of the following would be the BEST metric for the IT risk management process?

A.
Number of risk management action plans

B.
Percentage of critical assets with budgeted remedial

C.
Percentage of unresolved risk exposures

D.
Number of security incidents identified

Answer: B
Explanation:

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

QUESTION NO: 738

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

A.
Operational risk assessment

B.

Financial crime metrics

C.
Capacity management

D.
Business continuity management

Answer: D
Explanation:

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

QUESTION NO: 739

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.

Answer: C
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 NO: 740

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

A.
Encrypting first by receiver's private key and second by sender's public key

B.
Encrypting first by sender's private key and second by receiver's public key

C.
Encrypting first by sender's private key and second decrypting by sender's public key

D.
Encrypting first by sender's public key and second by receiver's private key

Answer: B
Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and. second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

QUESTION NO: 741

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.

Answer: C
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 NO: 742

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

A.
verify the decision with the business units.

B.
check the system's risk analysis.

C.
recommend update after post implementation review.

D.
request an audit review.

Answer: A
Explanation:

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

QUESTION NO: 743

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

A.
Denial of service (DoS) attacks

B.
Traffic sniffing

C.
Virus infections

D.
IP address spoofing

Answer: B
Explanation:

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

QUESTION NO: 744

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

A.
access to inappropriate sites.

B.
downloading malicious code.

C.
violation of copyright laws.

D.

disruption of Internet access.

Answer: D

Explanation:

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

QUESTION NO: 745

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.

Answer: A

Explanation:

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

QUESTION NO: 746

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

A.
Testing

B.
Initiation

C.
Design

D.
Development

Answer: C
Explanation:

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

QUESTION NO: 747

The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

A.
service level monitoring.

B.
penetration testing.

C.
periodically auditing.

D.
security awareness training.

Answer: C

Explanation:

Regular audit exercise can spot any gap in the information security compliance. Service level monitoring can only pinpoint operational issues in the organization's operational environment. Penetration testing can identify security vulnerability but cannot ensure information compliance Training can increase users' awareness on the information security policy, but is not more effective than auditing.

QUESTION NO: 748

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

A.
a strong authentication.

B.
IP antispoofing filtering.

C.
network encryption protocol.

D.
access lists of trusted devices.

Answer: A

Explanation:

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

QUESTION NO: 749

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

A.
contribute cost-effective expertise not available internally.

B.
be made responsible for meeting the security program requirements.

C.
replace the dependence on internal resources.

D.
deliver more effectively on account of their knowledge.

Answer: A
Explanation:

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

QUESTION NO: 750

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

Answer: D

Explanation:

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

QUESTION NO: 751

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

Answer: A

Explanation:

QUESTION NO: 752

Which of the following is the **MOST** effective way for an information security manager to ensure that security is incorporated into an organization’s project development processes?

A.
Conduct security reviews during design, testing, and implementation.

B.
Integrate organization’s security requirements into project management.

C.
Develop good communications with the project management office.

D.
Participate in project initiation, approval, and funding.

Answer: A
Explanation:

QUESTION NO: 753

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

Answer: D
Explanation:

QUESTION NO: 754

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.

Answer: D
Explanation:

QUESTION NO: 755

Which of the following is **MOST** important to consider when developing a business continuity plan (BCP)?

A.
Disaster recovery plan (DRP)

B.
Business impact analysis (BIA)

C.
Incident management requirements

D.
Business communication plan

Answer: B
Explanation:

QUESTION NO: 756

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

Answer: A
Explanation:

QUESTION NO: 757

Which of the following should provide the **PRIMARY** justification to approve the implementation of a disaster recovery (DR) site on the recommendation of an external audit report?

A.
Cost-benefit analysis

B.
Recovery time objectives (RTOs)

C.
Security controls at the DR site

D.
Regulatory requirements

Answer: A
Explanation:

QUESTION NO: 758

An information security manager has been tasked with implementing a security awareness training program. Which of the following will have the **MOST** influence on the effectiveness of this program?

A.
Obtaining buy-in from senior management

B.
Tailoring the training to the organization’s environment

C.
Obtaining buy-in from end users

D.
Basing the training program on industry best practices

Answer: C
Explanation:

Topic 4, INFORMATION SECURITY PROGRAM MANAGEMENT

QUESTION NO: 759

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

Answer: D
Explanation:

QUESTION NO: 760

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

Answer: D
Explanation:

QUESTION NO: 761

When developing security standards, which of the following would be MOST appropriate to include?

A.
Accountability for licenses

B.
Acceptable use of IT assets

C.
Operating system requirements

D.
Inventory management

Answer: B
Explanation:

QUESTION NO: 762

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.

Answer: D
Explanation:

QUESTION NO: 763

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.

Answer: C
Explanation:

QUESTION NO: 764

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

Answer: B
Explanation:

QUESTION NO: 765

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

Answer: A
Explanation:

QUESTION NO: 766

A data-hosting organization’s data center houses servers, applications, and data for a large number of geographically dispersed customers. Which of the following strategies would be the **BEST** approach for developing a physical access control policy for the organization?

A.
Design single sign-on or federated access.

B.
Conduct a risk assessment to determine security risks and mitigating controls.

C.
Develop access control requirements for each system and application.

D.
Review customers’ security policies.

Answer: B
Explanation:

QUESTION NO: 767

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.

Answer: A
Explanation:

QUESTION NO: 768

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

Answer: B

Explanation:

QUESTION NO: 769

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.

Answer: D

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

QUESTION NO: 770

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

Answer: D
Explanation:

QUESTION NO: 771

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.

Answer: D
Explanation:

QUESTION NO: 772

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

Answer: D
Explanation:

QUESTION NO: 773

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

Answer: A
Explanation:

QUESTION NO: 774

An organization has a policy in which all criminal activity is prosecuted. What is **MOST** important for the information security manager to ensure when an employee is suspected of using a company computer to commit fraud?

A.

The forensics process is immediately initiated.

B.
The incident response plan is initiated.

C.
The employee’s log files are backed-up.

D.
Senior management is informed of the situation.

Answer: C
Explanation:

QUESTION NO: 775

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.

Answer: C
Explanation:

QUESTION NO: 776

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

Answer: A
Explanation:

QUESTION NO: 777

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.

Answer: C
Explanation:

QUESTION NO: 778

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should **FIRST**:

A.
change the password policy to improve the customer experience.

B.
research alternative secure methods of identity verification.

C.
evaluate the impact of the customer's experience on business revenue.

D.
recommend implementing two-factor authentication.

Answer: B
Explanation:

QUESTION NO: 779

The **PRIMARY** reason for creating a business case when proposing an information security project is to:

A.
establish the value of the project in relation to business objectives.

B.
establish the value of the project with regard to regulatory compliance.

C.
ensure relevant business parties are involved in the project.

D.
ensure comprehensive security controls are identified.

Answer: A
Explanation:

QUESTION NO: 780

Which of the following will **BEST** help to proactively prevent the exploitation of vulnerabilities in operating system software?

A.
Patch management

B.
Threat management

C.
Intrusion detection system

D.
Anti-virus software

Answer: A

Explanation:

QUESTION NO: 781

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

Answer: D

Explanation:

QUESTION NO: 782

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

Answer: A
Explanation:

QUESTION NO: 783

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

Answer: B
Explanation:

QUESTION NO: 784

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.

Answer: D
Explanation:

QUESTION NO: 785

Segregation of duties is a security control **PRIMARILY** used to:

A.
establish dual check.

B.
establish hierarchy.

C.
limit malicious behavior.

D.
decentralize operations.

Answer: C
Explanation:

QUESTION NO: 786

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.

Answer: B

Explanation:

QUESTION NO: 787

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.

Answer: C

Explanation:

QUESTION NO: 788

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.

Answer: C
Explanation:

QUESTION NO: 789

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.

Answer: D
Explanation:

QUESTION NO: 790

The **PRIMARY** reason for using information security metrics is to:

A.

achieve senior management commitment.

B.
ensure alignment with corporate requirements.

C.
adhere to legal and regulatory requirements.

D.
monitor the effectiveness of controls.

Answer: D
Explanation:

QUESTION NO: 791

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

Answer: B
Explanation:

QUESTION NO: 792

Which of the following is the **BEST** defense against distributed denial of service (DDoS) attacks?

A.
Multiple and redundant paths

B.
Well-configured routers and firewalls

C.
Regular patching

D.
Intruder-detection lockout

Answer: B

Explanation:

QUESTION NO: 793

Which of the following function is the MOST critical when initiating the removal of system access for terminated employees?

A.
Human resources

B.
Legal

C.
Help desk

D.
Information security

Answer: D

Explanation:

QUESTION NO: 794

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

Answer: A
Explanation:

QUESTION NO: 795

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

Answer: C
Explanation:

QUESTION NO: 796

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

Answer: D
Explanation:

QUESTION NO: 797

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.

Answer: D
Explanation:

QUESTION NO: 798

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

Answer: A
Explanation:

QUESTION NO: 799

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.

Answer: C
Explanation:

QUESTION NO: 800

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

Answer: C
Explanation:

QUESTION NO: 801

Which of the following is the **PRIMARY** benefit of implementing a maturity model for information security management?

A.
Information security management costs will be optimized.

B.
Information security strategy will be in line with industry best practice.

C.
Gaps between current and desirable levels will be addressed.

D.
Staff awareness of information security compliance will be promoted.

Answer: C
Explanation:

QUESTION NO: 802

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

Answer: A
Explanation:

QUESTION NO: 803

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.

Answer: D
Explanation:

QUESTION NO: 804

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

Answer: C
Explanation:

QUESTION NO: 805

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.

Answer: D
Explanation:

QUESTION NO: 806

A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's **FIRST** course of action?

A.
Review the current security policy.

B.

Inform senior management of the new regulation.

C.
Update the security incident management process.

D.
Determine impact to the business.

Answer: A
Explanation:

QUESTION NO: 807

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.

Answer: A
Explanation:

QUESTION NO: 808

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.

Answer: B

Explanation:

QUESTION NO: 809

A multinational organization wants to monitor outbound traffic for data leakage from the use of unapproved cloud services. Which of the following should be the information security manager's **GREATEST** consideration when implementing this control?

A.

Security of cloud services

B.

Data privacy regulations

C.

Resistance from business users

D.

Allocation of monitoring resources

Answer: B

Explanation:

QUESTION NO: 810

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.

Answer: A

Explanation:

QUESTION NO: 811

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

Answer: D

Explanation:

QUESTION NO: 812

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.

Answer: D
Explanation:

QUESTION NO: 813

The **PRIMARY** advantage of single sign-on (SSO) is that it will:

A.
support multiple authentication mechanisms.

B.
increase the security related applications.

C.
strengthen user password.

D.
increase efficiency of access management.

Answer: D
Explanation:

QUESTION NO: 814

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.

Answer: B
Explanation:

QUESTION NO: 815

Which of the following architectures for e-business **BEST** ensures high availability?

A.
Availability of an adjacent hot site and a standby server with mirrored copies of critical data

B.
Intelligent middleware to direct transactions from a downed system to an alternative

C.
A single point of entry allowing transactions to be received and processed quickly

D.
Automatic failover to the web site of another e-business that meets the user’s needs

Answer: D
Explanation:

QUESTION NO: 816

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.

Answer: D
Explanation:

QUESTION NO: 817

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the **MOST** important action of the information security manager?

A.
Follow the outsourcer's response plan.

B.
Alert the appropriate law enforcement authorities.

C.
Refer to the organization's response plan.

D.
Notify the outsourcer of the privacy breach.

Answer: D
Explanation:

QUESTION NO: 818

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

Answer: A
Explanation:

QUESTION NO: 819

What of the following is **MOST** important to include in an information security policy?

A.
Maturity levels

B.
Best practices

C.
Management objectives

D.
Baselines

Answer: C
Explanation:

QUESTION NO: 820

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

Answer: A
Explanation:

QUESTION NO: 821

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.

Answer: D
Explanation:

QUESTION NO: 822

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.

Answer: C
Explanation:

QUESTION NO: 823

A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is **MOST** important to ensure:

A.
data sharing complies with local laws and regulations at both locations.

B.
data is encrypted in transit and at rest.

C.
a nondisclosure agreement is signed.

D.
risk coverage is split between the two locations sharing data.

Answer: A
Explanation:

QUESTION NO: 824

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.

Answer: D
Explanation:

QUESTION NO: 825

An information security manager is reviewing the impact of a regulation on the organization’s human resources system. The **NEXT** course of action should be to:

A.
perform a gap analysis of compliance requirements.

B.
assess the penalties for non-compliance.

C.
review the organization’s most recent audit report.

D.
determine the cost of compliance.

Answer: A
Explanation:

QUESTION NO: 826

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

Answer: A
Explanation:

QUESTION NO: 827

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

Answer: D
Explanation:

QUESTION NO: 828

An organization wants to integrate information security into its human resource management processes. Which of the following should be the **FIRST** step?

A.
Evaluate the cost of information security integration

B.
Assess the business objectives of the processes

C.
Identify information security risk associated with the processes

D.
Benchmark the processes with best practice to identify gaps

Answer: B
Explanation:

QUESTION NO: 829

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

Answer: C
Explanation:

QUESTION NO: 830

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

Answer: D
Explanation:

QUESTION NO: 831

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

Answer: A
Reference: https://searchdisasterrecovery.techtarget.com/answer/Whats-the-difference-between-a-hot-site-and-cold-site-for-disaster-recovery

QUESTION NO: 832

Which of the following messages would be **MOST** effective in obtaining senior management's commitment to information security management?

A.
Effective security eliminates risk to the business.

B.

Adopt a recognized framework with metrics.

C.
Security is a business product and not a process.

D.
Security supports and protects the business.

Answer: A
Explanation:

QUESTION NO: 833

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

Answer: B
Explanation:

QUESTION NO: 834

Which of the following presents the **GREATEST** challenge in calculating return on investment (ROI) in the security environment?

A.
Number of incidents cannot be predetermined.

B.

Project cost overruns cannot be anticipated.

C.
Cost of security tools is difficult to estimate.

D.
Costs of security incidents cannot be estimated.

Answer: A
Explanation:

QUESTION NO: 835

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

Answer: B
Explanation:

QUESTION NO: 836

Which of the following is the **MOST** important driver when developing an effective information security strategy?

A.
Information security standards

B.
Compliance requirements

C.
Benchmarking reports

D.
Security audit reports

Answer: A
Explanation:

QUESTION NO: 837

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

Answer: A
Explanation:

QUESTION NO: 838

Which of the following would **BEST** help to identify vulnerabilities introduced by changes to an organization’s technical infrastructure?

A.
An intrusion detection system

B.

Established security baselines

C.
Penetration testing

D.
Log aggregation and correlation

Answer: C
Explanation:

QUESTION NO: 839

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.

Answer: D
Explanation:

QUESTION NO: 840

In order to ensure separation of duties, which of the following activities is **BEST** performed by someone other than the system administrator?

A.
Deleting system logs

B.

Using system utilities

C.
Monitoring system utilization

D.
Defining system recovery procedures

Answer: A
Explanation:

QUESTION NO: 841

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

Answer: D
Explanation:

QUESTION NO: 842

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

Answer: C
Explanation:

QUESTION NO: 843

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.

Answer: C
Explanation:

QUESTION NO: 844

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

Answer: B
Explanation:

QUESTION NO: 845

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

Answer: D
Explanation:

QUESTION NO: 846

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

Answer: D

Explanation:

QUESTION NO: 847

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.

Answer: A

Explanation:

QUESTION NO: 848

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

Answer: A

Explanation:

QUESTION NO: 849

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.

Answer: D

Explanation:

QUESTION NO: 850

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).

Answer: B
Explanation:

QUESTION NO: 851

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.

Answer: A
Explanation:

QUESTION NO: 852

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

Answer: B
Explanation:

QUESTION NO: 853

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

Answer: A
Explanation:

QUESTION NO: 854

Senior management asks the information security manager for justification before approving the acquisition of a new intrusion detection system (IDS). The **BEST** course of action is to provide:

A.
documented industry best practices

B.
a gap analysis against the new IDS controls.

C.
a business case.

D.

a business impact analysis (BIA).

Answer: C

Explanation:

QUESTION NO: 855

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.

Answer: B

Explanation:

QUESTION NO: 856

Which of the following will **BEST** enable an effective information asset classification process?

A.

Reviewing the recovery time objective (RTO) requirements of the asset

B.

Analyzing audit findings

C.

Including security requirements in the classification process

D.

Assigning ownership

Answer: C

Explanation:

QUESTION NO: 857

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

Answer: D

Explanation:

QUESTION NO: 858

Which of the following should be the **MOST** important criteria when defining data retention policies?

A.
Capacity requirements

B.
Audit findings

C.
Regulatory requirements

D.

Industry best practices

Answer: C

Explanation:

QUESTION NO: 859

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

Answer: D

Explanation:

QUESTION NO: 860

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

Answer: D
Explanation:

QUESTION NO: 861

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.

Answer: A
Explanation:

QUESTION NO: 862

Failure to include information security requirements within the build/buy decision would **MOST** likely result in the need for:

A.
compensating controls in the operational environment.

B.
commercial product compliance with corporate standards.

C.
more stringent source programming standards.

D.
security scanning of operational platforms.

Answer: A
Explanation:

QUESTION NO: 863

A business impact analysis should be periodically executed **PRIMARILY** to:

A.
validate vulnerabilities on environmental changes.

B.
analyze the importance of assets.

C.
verify the effectiveness of controls.

D.
check compliance with regulations.

Answer: A
Explanation:

QUESTION NO: 864

The **GREATEST** benefit resulting from well-documented information security procedures is that they:

A.
ensure that security policies are consistently applied.

B.
ensure that critical processes can be followed by temporary staff.

C.
facilitate security training of new staff.

D.

provide a basis for auditing security practices.

Answer: A

Explanation:

QUESTION NO: 865

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

Answer: C

Explanation:

QUESTION NO: 866

Reviewing security objectives and ensuring the integration of security across business units is **PRIMARILY** the focus of the:

A.
executive management

B.
chief information security officer (CISO)

C.
board of directors

D.

steering committee.

Answer: B

Explanation:

QUESTION NO: 867

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

Answer: B

Explanation:

QUESTION NO: 868

Labeling information according to its security classification:

A.
enhances the likelihood of people handling information securely.

B.
reduces the number and type of countermeasures required.

C.
reduces the need to identify baseline controls for each classification.

D.
affects the consequences if information is handled insecurely.

Answer: D

Explanation:

QUESTION NO: 869

Meeting which of the following security objectives **BEST** ensures that information is protected against unauthorized disclosure?

A.
Authenticity

B.
Confidentiality

C.
Nonrepudiation

D.
Integrity

Answer: B

Explanation:

QUESTION NO: 870

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.

Answer: D

Explanation:

QUESTION NO: 871

Key systems necessary for branch operations reside at corporate headquarters. Branch A is negotiating with a third party to provide disaster recovery facilities.

Which of the following contract terms would be the MOST significant concern?

A.
The hot site for the branch may have to be shared.

B.
Connectivity is not provided from the hot site to corporate headquarters.

C.
Penalty clauses for nonperformance are not included in contract.

D.
The right to audit the hot site is not provided in the contract.

Answer: B

Explanation:

QUESTION NO: 872

A regulatory organization sends an email to an information security manager warning of an impending cyber-attack. The information security manager should **FIRST**:

A.
validate the authenticity of the alert

B.
determine whether the attack is in progress

C.
alert the network operations center

D.

reply asking for more details

Answer: A

Explanation:

QUESTION NO: 873

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.

Answer: B

Explanation:

QUESTION NO: 874

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

Answer: C

Explanation:

QUESTION NO: 875

Which of the following is the **PRIMARY** reason social media has become a popular target for attack?

A.
The prevalence of strong perimeter.

B.
The reduced effectiveness of access controls.

C.
The element of trust created by social media.

D.
The accessibility of social media from multiple locations.

Answer: D

Explanation:

QUESTION NO: 876

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.

Answer: C
Explanation:

QUESTION NO: 877

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

Answer: B
Explanation:

QUESTION NO: 878

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

Answer: C

Explanation:

QUESTION NO: 879

To ensure appropriate control of information processed in IT systems, security safeguards should be based **PRIMARILY** on:

A.

established guidelines

B.

criteria consistent with classification levels

C.

efficient technical processing considerations

D.

overall IT capacity and operational constraints

Answer: A

Explanation:

QUESTION NO: 880

The **PRIMARY** reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

A.

maintain an accurate record of users' access rights.

B.

serve as evidence of security awareness training.

C.

maintain compliance with industry best practices.

D.
assign accountability for transactions made with the user’s ID.

Answer: A
Explanation:

QUESTION NO: 881

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.

Answer: A
Explanation:

QUESTION NO: 882

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.

Answer: A
Explanation:

QUESTION NO: 883

An information security manager has researched several options for handling ongoing security concerns and will be presenting these solutions to business managers. Which of the following will **BEST** enable business managers to make an informed decision?

A.
Business impact analysis (BIA)

B.
Cost-benefit analysis

C.
Risk analysis

D.
Gap analysis

Answer: A
Explanation:

QUESTION NO: 884

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

Answer: D
Explanation:

QUESTION NO: 885

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)

Answer: C
Explanation:

QUESTION NO: 886

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

Answer: B

Explanation:

QUESTION NO: 887

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

Answer: C

Explanation:

QUESTION NO: 888

Which of the following would be the information security manager’s **BEST** course of action to gain approval for investment in a technical control?

A.

Perform a cost-benefit analysis.

B.

Conduct a risk assessment.

C.

Calculate the exposure factor.

D.

Conduct a business impact analysis (BIA).

Answer: D

Explanation:

QUESTION NO: 889

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.

Answer: A

Explanation:

QUESTION NO: 890

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.

Answer: D

Explanation:

QUESTION NO: 891

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.

Answer: A

Explanation:

QUESTION NO: 892

Which of the following is the **MOST** important consideration when selecting members for an information security steering committee?

A.
Cross-functional composition

B.
Information security expertise

C.
Tenure in the organization

D.
Business expertise

Answer: A

Explanation:

QUESTION NO: 893

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

Answer: A

Explanation:

QUESTION NO: 894

Meeting which of the following security objectives **BEST** ensures that information is protected against unauthorized modification?

A.
Authenticity

B.
Availability

C.
Confidentiality

D.
Integrity

Answer: D

Explanation:

QUESTION NO: 895

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.

Answer: A

Explanation:

QUESTION NO: 896

Which of the following should be the PRIMARY basis for an information security strategy?

A.
The organization’s vision and mission.

B.
Information security policies.

C.
Results of a comprehensive gap analysis.

D.
Audit and regulatory requirements.

Answer: A

Explanation:

QUESTION NO: 897

Which of the following is an example of a vulnerability?

A.
Natural disasters

B.
Defective software

C.
Ransomware

D.
Unauthorized users

Answer: B

Explanation:

QUESTION NO: 898

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.

Answer: A

Explanation:

QUESTION NO: 899

Which of the following is the **MOST** important reason to monitor information risk on a continuous basis?

A.
The risk profile can change over time.

B.
The effectiveness of controls can be verified.

C.
The cost of controls can be minimized.

D.
Risk assessment errors can be identified.

Answer: A

Explanation:

QUESTION NO: 900

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

Answer: A

Explanation:

QUESTION NO: 901

The PRIMARY purpose of vulnerability assessments is to:

A.
determine the impact of potential threats.

B.
test intrusion detection systems (IDS) and response procedures.

C.
provide clear evidence that the system is sufficiently secure.

D.
detect deficiencies that could lead to a system compromise.

Answer: D

Explanation:

QUESTION NO: 902

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

Answer: A

Explanation:

QUESTION NO: 903

The recovery point objective (RPO) is required in which of the following?

A.
Information security plan

B.
Incident response plan

C.
Business continuity plan

D.
Disaster recovery plan

Answer: C

Explanation:

QUESTION NO: 904

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.

Answer: C

Explanation:

QUESTION NO: 905

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

Answer: D
Explanation:

QUESTION NO: 906

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

Answer: B
Explanation:

QUESTION NO: 907

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

Answer: C
Explanation:

QUESTION NO: 908

Which of the following would **BEST** help to ensure an organization’s security program is aligned with business objectives?

A.
Security policies are reviewed and approved by the chief information officer.

B.
The security strategy is reviewed and approved by the organization’s executive committee.

C.
The organization’s board of directors includes a dedicated information security specialist.

D.
Project managers receive annual information security awareness training.

Answer: B
Explanation:

QUESTION NO: 909

Which of the following will **MOST** effectively minimize the chance of inadvertent disclosure of confidential information?

A.
Following the principle of least privilege

B.
Restricting the use of removable media

C.
Applying data classification rules

D.
Enforcing penalties for security policy violations

Answer: C
Explanation:

QUESTION NO: 910

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

Answer: A
Explanation:

QUESTION NO: 911

Which of the following is the **PRIMARY** benefit of using agentless endpoint security solutions?

A.
Decreased network bandwidth usage

B.
Decreased administration

C.
Increased resiliency

D.
More comprehensive information results

Answer: B
Explanation:

QUESTION NO: 912

Which of the following **MOST** efficiently ensures the proper installation of a firewall policy that restricts a small group of internal IP addresses from accessing the Internet?

A.
A connectivity test from the restricted host

B.
A simulated denial of service attack against the firewall

C.
A port scan of the firewall from an external source

D.
A review of the current firewall configuration

Answer: A
Explanation:

QUESTION NO: 913

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

Answer: D
Explanation:

QUESTION NO: 914

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.

Answer: B
Explanation:

QUESTION NO: 915

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.

Answer: A
Explanation:

QUESTION NO: 916

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

Answer: A
Explanation:

QUESTION NO: 917

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.

Answer: A
Explanation:

QUESTION NO: 918

The **BEST** way to identify the criticality of systems to the business is through:

A.
a threat assessment.

B.
an asset classification.

C.
a vulnerability assessment.

D.
an impact assessment.

Answer: B
Explanation:

QUESTION NO: 919

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

Answer: A
Explanation:

QUESTION NO: 920

Which of the following is the **BEST** way to identify the potential impact of a successful attack on an organization's mission critical applications?

A.
Conduct penetration testing.

B.
Execute regular vulnerability scans.

C.
Perform independent code review.

D.
Perform application vulnerability review.

Answer: A
Explanation:

QUESTION NO: 921

Which of the following is the **BEST** method to defend against social engineering attacks?

A.
Periodically perform antivirus scans to identify malware.

B.

Communicate guidelines to limit information posted to public sites.

C.

Employ the use of a web-content filtering solution.

D.

Monitor for unauthorized access attempts and failed logins.

Answer: C

Explanation:

QUESTION NO: 922

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.

Answer: D

Explanation:

QUESTION NO: 923

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

Answer: A

Explanation:

QUESTION NO: 924

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

Answer: D

Explanation:

QUESTION NO: 925

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

Answer: B

Explanation:

QUESTION NO: 926

During the security review of a legacy business application, it was discovered that sensitive client data is not encrypted in storage, which does not comply with the organization's information security policy. Which of the following would be the information security manager's **BEST** course of action?

A.
Implement encryption on client data.

B.
Report the noncompliance to senior management.

C.
Analyze compensating controls and assess the associated risk.

D.
Determine the cost of encryption and discuss with the application owner.

Answer: C

Explanation:

QUESTION NO: 927

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

A.
perform penetration testing.

B.
establish security baselines.

C.
implement vendor default settings.

D.
link policies to an independent standard.

Answer: B
Explanation:

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

QUESTION NO: 928

A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

A.
User

B.
Network

C.
Operations

D.
Database

Answer: A
Explanation:

As owners of the system, user management signoff is the most important. If a system does not meet the needs of the business, then it has not met its primary objective. The needs of network, operations and database management are secondary to the needs of the business.

QUESTION NO: 929

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

A.
distribute printed copies to all employees.

B.
perform periodic reviews for compliance.

C.
include escalating penalties for noncompliance.

D.
establish an anonymous hotline to report policy abuses.

Answer: B
Explanation:

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

QUESTION NO: 930

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

A.
system developer.

B.
information security manager.

C.

steering committee.

D.
system data owner.

Answer: D
Explanation:

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

QUESTION NO: 931

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

Answer: B
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 NO: 932

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

A.
Adequate security policies and procedures

B.
Periodic compliance reviews

C.
Security steering committees

D.
Security awareness campaigns

Answer: D

Explanation:

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

QUESTION NO: 933

The BEST way to ensure that an external service provider complies with organizational security policies is to:

A.
Explicitly include the service provider in the security policies.

B.
Receive acknowledgment in writing stating the provider has read all policies.

C.
Cross-reference to policies in the service level agreement

D.

Perform periodic reviews of the service provider.

Answer: D

Explanation:

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

QUESTION NO: 934

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

A.
loaded onto an isolated test machine.

B.
decompiled to check for malicious code.

C.
validated to ensure its authenticity.

D.
copied onto write-once media to prevent tampering.

Answer: C

Explanation:

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

QUESTION NO: 935

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

A.
Applying patches

B.
Changing access rules

C.
Upgrading hardware

D.
Backing up files

Answer: B
Explanation:

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

QUESTION NO: 936

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

Answer: B
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 NO: 937

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

Answer: A
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 NO: 938

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.

Answer: D
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 NO: 939

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

A.
User

B.
Security

C.
Operations

D.
Database

Answer: A
Explanation:

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

QUESTION NO: 940

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.

Answer: B
Explanation:

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

QUESTION NO: 941

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.

Answer: B

Explanation:

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

QUESTION NO: 942

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

Answer: C

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 NO: 943

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

A.

Locally managed file server

B.
Enterprise data warehouse

C.
Load-balanced, web server cluster

D.
Centrally managed data switch

Answer: A
Explanation:

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

QUESTION NO: 944

Nonrepudiation can BEST be assured by using:

A.
delivery path tracing.

B.
reverse lookup translation.

C.
out-of-hand channels.

D.
digital signatures.

Answer: D
Explanation:

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

QUESTION NO: 945

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.

Answer: D
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 NO: 946

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

A.
Database management

B.
Tape backup management

C.
Configuration management

D.
Incident response management

Answer: C

Explanation:

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

QUESTION NO: 947

Security policies should be aligned MOST closely with:

A.
industry' best practices.

B.
organizational needs.

C.
generally accepted standards.

D.
local laws and regulations.

Answer: B

Explanation:

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

QUESTION NO: 948

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.

Answer: A
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 NO: 949

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.

Answer: C
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 NO: 950

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.

Answer: C
Explanation:

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

QUESTION NO: 951

What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

A.
Perform periodic penetration testing

B.
Establish minimum security baselines

C.
Implement vendor default settings

D.
Install a honeypot on the network

Answer: D

Explanation:

Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed sporadically. Vendor default settings are not effective.

QUESTION NO: 952

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

A.
User ad hoc reporting is not logged

B.
Network traffic is through a single switch

C.
Operating system (OS) security patches have not been applied

D.
Database security defaults to ERP settings

Answer: C

Explanation:

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

QUESTION NO: 953

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

Answer: B

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 NO: 954

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

Answer: C

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 NO: 955

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

A.
System analyst

B.
Quality control manager

C.
Process owner

D.
Information security manager

Answer: C

Explanation:

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

QUESTION NO: 956

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

A.
Explicitly refer to contractors in the security standards

B.
Have the contractors acknowledge in writing the security policies

C.
Create penalties for noncompliance in the contracting agreement

D.
Perform periodic security reviews of the contractors

Answer: D
Explanation:

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

QUESTION NO: 957

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

A.
Applying patches

B.
Changing access rules

C.
Upgrading hardware

D.
Backing up files

Answer: D
Explanation:

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

QUESTION NO: 958

Security awareness training should be provided to new employees:

A.
on an as-needed basis.

B.
during system user training.

C.
before they have access to data.

D.
along with department staff.

Answer: C
Explanation:

Security awareness training should occur before access is granted to ensure the new employee understands that security is part of the system and business process. All other choices imply that security awareness training is delivered subsequent to the granting of system access, which may place security as a secondary step.

QUESTION NO: 959

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

A.
Trace change control requests to operating system (OS) patch logs

B.

Trace OS patch logs to OS vendor's update documentation

C.
Trace OS patch logs to change control requests

D.
Review change control documentation for key servers

Answer: C
Explanation:

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

QUESTION NO: 960

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.

Answer: C
Explanation:

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

QUESTION NO: 961

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.

Answer: B
Explanation:

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

QUESTION NO: 962

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

A.
Preemployment screening

B.
Close monitoring of users

C.
Periodic awareness training

D.
Effective termination procedures

Answer: D
Explanation:

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

QUESTION NO: 963

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

A.
Data mining

B.
Network mapping

C.
Intrusion Detection System (IDS)

D.
Customer data

Answer: B
Explanation:

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

QUESTION NO: 964

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

A.
Support of business objectives

B.
Security metrics

C.
Security deliverables

D.
Process improvement models

Answer: A

Explanation:

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

QUESTION NO: 965

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.

Answer: B
Explanation:

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

QUESTION NO: 966

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.

Answer: C
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 NO: 967

Which of the following **BEST** indicates senior management support for an information security program?

A.
Detailed information security policies are established and regularly reviewed.

B.
The information security manager meets regularly with the lines of business.

C.
Key performance indicators (KPIs) are defined for the information security program.

D.
Risk assessments are conducted frequently by the information security team.

Answer: C

Explanation:

QUESTION NO: 968

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.

Answer: C

Explanation:

QUESTION NO: 969

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.

Answer: D
Explanation:

QUESTION NO: 970

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

Answer: C
Explanation:

QUESTION NO: 971

Which of the following would be the **BEST** way for a company to reduce the risk of data loss resulting from employee-owned devices accessing the corporate email system?

A.
Link the bring-your-own-device (BYOD) policy to the existing staff disciplinary policy.

B.
Require employees to undergo training before permitting access to the corporate email service.

C.
Require employees to install a reputable mobile anti-virus solution on their personal devices.

D.
Use a mobile device management (MDM) solution to isolate the local corporate email storage.

Answer: D
Explanation:

QUESTION NO: 972

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

Answer: A
Explanation:

QUESTION NO: 973

Which of the following is the **MOST** effective defense against spear phishing attacks?

A.
Unified threat management

B.
Web filtering

C.
Anti-spam solutions

D.
User awareness training

Answer: D
Explanation:

QUESTION NO: 974

Which of the following is **MOST** important to evaluate after completing a risk action plan?

A.
Threat profile

B.
Inherent risk

C.
Residual risk

D.
Vulnerability landscape

Answer: A
Explanation:

QUESTION NO: 975

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.

Answer: D
Explanation:

QUESTION NO: 976

A newly hired information security manager discovers that the cleanup of accounts for terminated employees happens only once a year.

Which of the following should be the information security manager’s **FIRST** course of action?

A.
Design and document a new process.

B.
Update the security policy.

C.
Perform a risk assessment.

D.
Report the issue to senior management.

Answer: C
Explanation:

QUESTION NO: 977

A multinational organization wants to ensure its privacy program appropriately addresses privacy risk throughout its operations.

Which of the following would be of **MOST** concern to senior management?

A.
The organization uses a decentralized privacy governance structure.

B.
Privacy policies are only reviewed annually.

C.
The organization does not have a dedicated privacy officer.

D.
The privacy program does not include a formal training component.

Answer: D
Explanation:

QUESTION NO: 978

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.

Answer: D
Explanation:

QUESTION NO: 979

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.

Answer: A
Explanation:

QUESTION NO: 980

Which of the following is the **MOST** important outcome from vulnerability scanning?

A.
Prioritization of risks

B.
Information about steps necessary to hack the system

C.
Identification of back doors

D.
Verification that systems are properly configured

Answer: D
Explanation:

QUESTION NO: 981

Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered a significant exposure?

A.
Authentication server

B.
Web server

C.
Proxy server

D.
Intrusion detection server

Answer: A
Explanation:

QUESTION NO: 982

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

Answer: C
Explanation:

QUESTION NO: 983

In a large organization requesting outsourced services, which of the following contract clauses is **MOST** important to the information security manager?

A.
Compliance with security requirements

B.
Frequency of status reporting

C.
Nondisclosure clause

D.
Intellectual property (IP)

Answer: A
Explanation:

QUESTION NO: 984

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.

Answer: D
Explanation:

QUESTION NO: 985

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

Answer: D
Explanation:

QUESTION NO: 986

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.

Answer: A
Explanation:

QUESTION NO: 987

Which of the following is the **MOST** effective way to identify changes in an information security environment?

A.
Continuous monitoring

B.
Security baselining

C.
Annual risk assessments

D.
Business impact analysis

Answer: A
Explanation:

QUESTION NO: 988

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

Answer: B
Explanation:

QUESTION NO: 989

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.

Answer: C
Explanation:

QUESTION NO: 990

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.

Answer: D
Explanation:

QUESTION NO: 991

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.

Answer: D

Explanation:

QUESTION NO: 992

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

Answer: B

Explanation:

QUESTION NO: 993

Which of the following is the **BEST** way to sustain employee interest in information awareness in an organization?

A.
Ensuring a common security awareness program for all staff

B.
Relating security awareness programs to security policies

C.
Ensuring all staff are involved

D.
Using a variety of delivery methods

Answer: D
Explanation:

QUESTION NO: 994

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

Answer: C
Explanation:

QUESTION NO: 995

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.

Answer: D
Explanation:

QUESTION NO: 996

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

Answer: D
Explanation:

QUESTION NO: 997

What is the **BEST** way for a customer to authenticate an e-commerce vendor?

A.
Use a secure communications protocol for the connection.

B.
Verify the vendor’s certificate with a certificate authority.

C.
Request email verification of the order.

D.
Encrypt the order using the vendor’s private key.

Answer: B

Explanation:

QUESTION NO: 998

Which of the following would **BEST** enhance firewall security?

A.
Placing the firewall on a screened subnet

B.
Logging of security events

C.
Implementing change-control practices

D.
Providing dynamic address assignment

Answer: B

Explanation:

QUESTION NO: 999

Which of the following would provide nonrepudiation of electronic transactions?

A.
Two-factor authentication

B.
Periodic reaccreditations

C.
Third-party certificates

D.
Receipt acknowledgment

Answer: C
Explanation:

QUESTION NO: 1000

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.

Answer: B
Explanation:

QUESTION NO: 1001

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.

Answer: C

Explanation:

QUESTION NO: 1002

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

Answer: A

Explanation:

QUESTION NO: 1003

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)

Answer: B
Explanation:

QUESTION NO: 1004

Which of the following should be done **FIRST** when selecting performance metrics to report on the vendor risk management process?

A.
Review the confidentiality requirements.

B.
Identity the data owner.

C.
Select the data source.

D.
Identity the intended audience.

Answer: B
Explanation:

QUESTION NO: 1005

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.

Answer: A
Explanation:

QUESTION NO: 1006

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.

Answer: A
Explanation:

QUESTION NO: 1007

An information security manager learns of a new international standard related to information security.

Which of the following would be the **BEST** course of action?

A.
Review industry peers’ responses to the new standard.

B.
Consult with legal counsel on the standard’s applicability to regulations.

C.
Determine whether the organization can benefit from adopting the new standard.

D.
Perform a gap analysis between the new standard and existing practices.

Answer: C

Explanation:

QUESTION NO: 1008

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

Answer: B

Explanation:

QUESTION NO: 1009

Which of the following is **MOST** helpful to management in determining whether risks are within an organization’s tolerance level?

A.
Audit findings

B.
Heat map

C.
Penetration test results

D.
Maturity level

Answer: B
Explanation:

QUESTION NO: 1010

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

Answer: B
Explanation:

QUESTION NO: 1011

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.

Answer: D
Explanation:

QUESTION NO: 1012

Which of the following is **MOST** important when selecting a third-party security operations center?

A.
Indemnity clauses

B.
Independent controls assessment

C.
Incident response plans

D.
Business continuity plans

Answer: B
Explanation:

QUESTION NO: 1013

An information security manager learns users of an application are frequently using emergency elevated access privileges to process transactions.

Which of the following should be done **FIRST**?

A.
Request justification from the user’s managers for emergency access.

B.
Request the application administrator block all emergency access profiles.

C.
Update the frequency and usage of the emergency access profile in the policy.

D.
Review the security architecture of the application and recommend changes.

Answer: D
Explanation:

QUESTION NO: 1014

Which of the following is MOST critical to review when preparing to outsource a data repository to a cloud-based solution?

A.
Disaster recovery plan

B.
Identity and access management

C.
Vendor’s information security policy

D.
A risk assessment

Answer: C
Explanation:

QUESTION NO: 1015

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)

Answer: A
Explanation:

QUESTION NO: 1016

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

Answer: B
Explanation:

QUESTION NO: 1017

Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?

A.
Risk assessment

B.
Business impact analysis (BIA)

C.
Penetration testing

D.
Gap analysis

Answer: D
Explanation:

QUESTION NO: 1018

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

Answer: D
Explanation:

QUESTION NO: 1019

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

A.
Conduct a business impact analysis (BIA) and provide the report to management.

B.
Update the corporate mobile usage policy to prohibit texting.

C.
Stop providing mobile devices until the organization is able to implement controls.

D.
Include the topic of prohibited texting in security awareness training.

Answer: D
Explanation:

QUESTION NO: 1020

Which of the following is the BEST approach for determining the maturity level of an information security program?

A.
Evaluate key performance indicators (KPIs)

B.
Engage a third-party review

C.
Review internal audit results

D.
Perform a self-assessment

Answer: A
Explanation:

QUESTION NO: 1021

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

A.
using a secret key in conjunction with the hash algorithm

B.
requiring the recipient to use a different hash algorithm

C.
using the sender’s public key to encrypt the message

D.
generating hash output that is the same size as the original message

Answer: A
Explanation:

QUESTION NO: 1022

An organization’s marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risks assessment. Which of the following should be the MOST important consideration?

A.
The information to be exchanged

B.
Methods for transferring the information

C.
Reputations of the external marketing companies

D.
The security of the third-party cloud provider

Answer: B
Explanation:

QUESTION NO: 1023

What should the information security manager do FIRST when end users express that new security controls are too restrictive?

A.
Conduct a business impact analysis (BIA)

B.
Obtain process owner buy-in to remove the controls

C.
Perform a risk assessment on modifying the control environment

D.
Perform a cost-benefit analysis on modifying the control environment

Answer: C
Explanation:

QUESTION NO: 1024

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)

Answer: D
Explanation:

QUESTION NO: 1025

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

Answer: C
Explanation:

QUESTION NO: 1026

Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

A.
Requiring periodic self-assessments by the provider

B.
Evaluating the provider’s security incident response plan

C.
Continuous monitoring of an information security risk profile

D.
Ensuring the provider’s roles and responsibilities are established

Answer: C
Explanation:

QUESTION NO: 1027

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.

Answer: C

Explanation:

QUESTION NO: 1028

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

Answer: A

Explanation:

QUESTION NO: 1029

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

Answer: B

Explanation:

QUESTION NO: 1030

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

Answer: A

Explanation:

QUESTION NO: 1031

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

Answer: B
Explanation:

QUESTION NO: 1032

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

Answer: A
Explanation:

QUESTION NO: 1033

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

Answer: C
Explanation:

QUESTION NO: 1034

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

Answer: D
Explanation:

QUESTION NO: 1035

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

Answer: D
Explanation:

QUESTION NO: 1036

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

Answer: C
Explanation:

QUESTION NO: 1037

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

Answer: A
Explanation:

QUESTION NO: 1038

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

Answer: A
Explanation:

QUESTION NO: 1039

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

Answer: A
Explanation:

QUESTION NO: 1040

Which of the following MOST effectively prevents internal users from modifying sensitive data?

A.
Network segmentation

B.
Acceptable use policies

C.
Role-based access controls

D.
Multi-factor authentication

Answer: C
Explanation:

QUESTION NO: 1041

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

Answer: C

Explanation:

QUESTION NO: 1042

Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

A.
Holding periodic meetings with business owners

B.
Promoting security training

C.
Establishing a steering committee

D.
Creating communication channels

Answer: C

Explanation:

QUESTION NO: 1043

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

Answer: A
Explanation:

QUESTION NO: 1044

The selection of security controls is PRIMARILY linked to:

A.
best practices of similar organizations

B.
risk appetite of the organization

C.
regulatory requirements

D.
business impact assessment

Answer: B
Explanation:

QUESTION NO: 1045

Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization’s information security program?

A.
Right-to-audit clause

B.
Escalation paths

C.
Key performance indicators (KPIs)

D.
Termination language

Answer: C
Explanation:

QUESTION NO: 1046

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

Answer: B
Explanation:

QUESTION NO: 1047

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

Answer: D
Explanation:

QUESTION NO: 1048

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

Answer: A
Explanation:

QUESTION NO: 1049

An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST?

A.
Application owners

B.
Communications department

C.
Data owners

D.
Security operations team

Answer: D

Explanation:

QUESTION NO: 1050

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

Answer: B

Explanation:

QUESTION NO: 1051

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)

Answer: B
Explanation:

QUESTION NO: 1052

Which of the following is an example of a change to the external threat landscape?

A.
Infrastructure changes to the organization have been implemented

B.
Organizational security standards have been modified

C.
A commonly used encryption algorithm has been compromised

D.
New legislation has been enacted in a region where the organization does business

Answer: D
Explanation:

QUESTION NO: 1053

Which of the following roles should be PRIMARILY responsible for assigning sensitivity levels to an organization’s financial and payroll databases?

A.

Data owner

B.
Database administrator

C.
Systems administrator

D.
Information security manager

Answer: A
Explanation:

QUESTION NO: 1054

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

A.
the importance of the functional to be tested and the cost of testing

B.
the experience level of personnel and the function location

C.
prior testing results and the degree of detail of the business continuity plan

D.
manual processing capabilities and the test location

Answer: A
Explanation:

QUESTION NO: 1055

A policy has been established requiring users to install mobile device management (MDM) software on their personal devices. Which of the following would BEST mitigate the risk created by noncompliance with this policy?

A.
Issuing warnings and documenting noncompliance

B.
Requiring users to sign off on terms and conditions

C.
Issuing company-configured mobile devices

D.
Disabling remote access from the mobile device

Answer: D
Explanation:

QUESTION NO: 1056

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

Answer: A
Explanation:

QUESTION NO: 1057

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

Answer: B
Explanation:

QUESTION NO: 1058

Which of the following is MOST effective against system intrusions?

A.
Two-factor authentication

B.
Continuous monitoring

C.
Layered protection

D.
Penetration testing

Answer: C
Explanation:

QUESTION NO: 1059

What should be the information security manager’s MOST important consideration when planning a disaster recovery test?

A.
Documented escalation processes

B.
Organization-wide involvement

C.
Impact to production systems

D.
Stakeholder notification procedures

Answer: C
Explanation:

QUESTION NO: 1060

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

Answer: D
Explanation:

QUESTION NO: 1061

The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:

A.

security program priorities to achieve an accepted risk level

B.
level of compliance with internal policy

C.
assessed level of security risk at a particular point in time

D.
current and target security state for the business

Answer: D
Explanation:

QUESTION NO: 1062

Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

A.
Identifying risk mitigation options

B.
Identifying critical business processes

C.
Identifying key business risks

D.
Identifying the threat environment

Answer: C
Explanation:

QUESTION NO: 1063

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

Answer: D

Explanation:

QUESTION NO: 1064

The MOST important reason that security risk assessments should be conducted frequently throughout an organization is because:

A.

control effectiveness may weaken

B.

compliance with legal and regulatory standards should be reassessed

C.

controls should be regularly tested

D.

threats to the organization may change

Answer: D

Explanation:

QUESTION NO: 1065

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

Answer: A
Explanation:

QUESTION NO: 1066

Which of the following is the PRIMARY role of a data custodian?

A.
Validating information

B.
Processing information

C.
Classifying information

D.
Securing information

Answer: D
Explanation:

QUESTION NO: 1067

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.

Answer: D
Explanation:

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

QUESTION NO: 1068

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

A.
User passwords are not automatically expired

B.
All network traffic goes through a single switch

C.
User passwords are encoded but not encrypted

D.
All users reside on a single internal subnet

Answer: C
Explanation:

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

QUESTION NO: 1069

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

A.
Standards

B.
Guidelines

C.
Security metrics

D.
IT governance

Answer: A
Explanation:

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

QUESTION NO: 1070

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

A.
Direct reports to the chief information officer

B.
IT management and key business process owners

C.
Cross-section of end users and IT professionals

D.

Internal audit and corporate legal departments

Answer: B

Explanation:

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

QUESTION NO: 1071

Security audit reviews should PRIMARILY:

A.
ensure that controls operate as required.

B.
ensure that controls are cost-effective.

C.
focus on preventive controls.

D.
ensure controls are technologically current.

Answer: A

Explanation:

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

QUESTION NO: 1072

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

A.
Delivery path tracing

B.
Reverse lookup translation

C.
Out-of-band channels

D.
Digital signatures

Answer: C
Explanation:

Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting; in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

QUESTION NO: 1073

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

Answer: A
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 NO: 1074

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

A.
A higher number of false positives

B.
New attack methods will be missed

C.
Long duration probing will be missed

D.
Attack profiles can be easily spoofed

Answer: B
Explanation:

Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

QUESTION NO: 1075

Data owners are normally responsible for which of the following?

A.
Applying emergency changes to application data

B.

Administering security over database records

C.
Migrating application code changes to production

D.
Determining the level of application security required

Answer: D
Explanation:

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

QUESTION NO: 1076

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

Answer: B
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 NO: 1077

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

A.
Include password construction requirements in the security standards

B.
Require each user to acknowledge the password requirements

C.
Implement strict penalties for user noncompliance

D.
Enable system-enforced password configuration

Answer: D
Explanation:

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

QUESTION NO: 1078

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

A.
Batch patches into frequent server updates

B.
Initially load the patches on a test machine

C.
Set up servers to automatically download patches

D.
Automatically push all patches to the servers

Answer: B

Explanation:

Some patches can conflict with application code. For this reason, it is very important to first test all patches in a test environment to ensure that there are no conflicts with existing application systems. For this reason, choices C and D are incorrect as they advocate automatic updating. As for frequent server updates, this is an incomplete (vague) answer from the choices given.

QUESTION NO: 1079

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

A.
Virus signature files updates are applied to all servers every day

B.
Security access logs are reviewed within five business days

C.
Critical patches are applied within 24 hours of their release

D.
Security incidents are investigated within five business days

Answer: D

Explanation:

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

QUESTION NO: 1080

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.

Answer: C
Explanation:

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

QUESTION NO: 1081

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

Answer: C
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 NO: 1082

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

A.
Reduced number of security violation reports

B.
A quantitative evaluation to ensure user comprehension

C.
Increased interest in focus groups on security issues

D.
Increased number of security violation reports

Answer: B
Explanation:

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

QUESTION NO: 1083

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

Answer: D
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 NO: 1084

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

Answer: A
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 NO: 1085

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

A.
Signal strength

B.
Number of administrators

C.
Bandwidth

D.
Encryption strength

Answer: B
Explanation:

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

QUESTION NO: 1086

Good information security standards should:

A.
define precise and unambiguous allowable limits.

B.
describe the process for communicating violations.

C.
address high-level objectives of the organization.

D.
be updated frequently as new software is released.

Answer: A

Explanation:

A security standard should clearly state what is allowable; it should not change frequently. The process for communicating violations would be addressed by a security procedure, not a standard. High-level objectives of an organization would normally be addressed in a security policy.

QUESTION NO: 1087

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.

Answer: D

Explanation:

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

QUESTION NO: 1088

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.

Answer: C
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 NO: 1089

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

Answer: C
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 NO: 1090

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.

Answer: A
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 NO: 1091

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

A.
The number of false positives increases

B.
The number of false negatives increases

C.
Active probing is missed

D.
Attack profiles are ignored

Answer: A
Explanation:

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

QUESTION NO: 1092

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

Answer: C
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 NO: 1093

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

A.
Information security officer

B.
Security steering committee

C.
Data owner

D.
Data custodian

Answer: B
Explanation:

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

QUESTION NO: 1094

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

A.
authorized.

B.
applied.

C.
documented.

D.
tested.

Answer: A

Explanation:

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

QUESTION NO: 1095

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

A.
Research best practices

B.
Meet with stakeholders

C.
Establish change control procedures

D.
Identify critical systems

Answer: B

Explanation:

No new process will be successful unless it is adhered to by all stakeholders; to the extent stakeholders have input, they can be expected to follow the process. Without consensus agreement from the stakeholders, the scope of the research is too wide; input on the current environment is necessary to focus research effectively. It is premature to implement procedures without stakeholder consensus and research. Without knowing what the process will be the parameters to baseline are unknown as well.

QUESTION NO: 1096

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

Answer: A
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 NO: 1097

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

A.
User security procedures

B.
Business process flow

C.
IT security policy

D.
Regulatory requirements

Answer: C

Explanation:

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

QUESTION NO: 1098

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

A.
The right to conduct independent security reviews

B.
A legally binding data protection agreement

C.
Encryption between the organization and the provider

D.
A joint risk assessment of the system

Answer: A

Explanation:

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

QUESTION NO: 1099

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

A.
Card key door locks

B.
Photo identification

C.
Awareness training

D.
Biometric scanners

Answer: C
Explanation:

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

QUESTION NO: 1100

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

A.
ensure access to individual functions can be granted to individual users only.

B.
implement role-based access control in the application.

C.
enforce manual procedures ensuring separation of conflicting duties.

D.
create service accounts that can only be used by authorized team members.

Answer: B

Explanation:

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

QUESTION NO: 1101

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

A.
information security manager.

B.
data owner.

C.
data custodian.

D.
business management.

Answer: B

Explanation:

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

QUESTION NO: 1102

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.

Answer: A
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 NO: 1103

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.

Answer: C

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 NO: 1104

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

Answer: C

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 NO: 1105

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.

Answer: C
Explanation:

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

QUESTION NO: 1106

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

A.
an effective control over connectivity and continuity.

B.
a service level agreement (SLA) including code escrow.

C.
a business impact analysis (BIA).

D.
a third-party certification.

Answer: A
Explanation:

The principal risk focus is the connection procedures to maintain continuity in case of any contingency. Although an information security manager may be interested in the service level agreement (SLA), code escrow is not a concern. A business impact analysis (BIA) refers to contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

QUESTION NO: 1107

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

Answer: C
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 NO: 1108

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

Answer: D
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 NO: 1109

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

A.
Adequate budgetary support

B.
Centralized program management

C.
Top-down approach

D.
Experience of the awareness trainers

Answer: C
Explanation:

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

QUESTION NO: 1110

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

Answer: B
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 NO: 1111

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

A.
business process owners.

B.
the information security manager.

C.
the security steering committee.

D.
IT senior management.

Answer: D

Explanation:

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

QUESTION NO: 1112

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

Answer: A

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 NO: 1113

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.

Answer: C
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 NO: 1114

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

A.
Database administrator (DBA)

B.
Finance department management

C.
Information security manager

D.
IT department management

Answer: B
Explanation:

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

QUESTION NO: 1115

Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A.
Compromised customer information

B.
Unavailability of online transactions

C.
Theft of security tokens

D.
Theft of a Research and Development laptop

Answer: D
Explanation:

The research and development department is usually the most sensitive area of the pharmaceutical organization, Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical: therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

QUESTION NO: 1116

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

A.
The program's governance oversight mechanisms

B.
Information security periodicals and manuals

C.
The program's security architecture and design

D.
Training and certification of the information security team

Answer: A
Explanation:

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

QUESTION NO: 1117

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

A.
Security audit reports

B.
Balanced scorecard

C.
Capability maturity model (CMM)

D.
Systems and business security architecture

Answer: C
Explanation:

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

QUESTION NO: 1118

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

A.
Chief information officer (CIO)

B.
Chief financial officer (CFO)

C.
Information security manager

D.
Business unit management

Answer: C
Explanation:

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

QUESTION NO: 1119

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

A.
system administrator.

B.
security administrator.

C.
system developer.

D.
independent trusted source.

Answer: D

Explanation:

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

QUESTION NO: 1120

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

A.
Budget allocation

B.
Technical skills of staff

C.
User acceptance

D.
Password requirements

Answer: C

Explanation:

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

QUESTION NO: 1121

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

A.
Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans

B.
Periodic audits of the disaster recovery/business continuity plans

C.
Comprehensive walk-through testing

D.
Inclusion as a required step in the system life cycle process

Answer: D
Explanation:

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

QUESTION NO: 1122

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.

Answer: D
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 NO: 1123

To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

A.
Service level agreements (SLAs)

B.
Right to audit clause

C.
Intrusion detection system (IDS) services

D.
Spam filtering services

Answer: A
Explanation:

Service level agreements (SLA) will be most effective in ensuring that Internet service providers (ISPs) comply with expectations for service availability. Intrusion detection system (IDS) and spam filtering services would not mitigate (as directly) the potential for service interruptions. A right-to-audit clause would not be effective in mitigating the likelihood of a service interruption.

QUESTION NO: 1124

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.

Answer: B
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 NO: 1125

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.

Answer: D
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 NO: 1126

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

Answer: A
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 NO: 1127

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

A.
Mantrap

B.
Biometric lock

C.
Closed-circuit television (CCTV)

D.
Security guard

Answer: B

Explanation:

A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

QUESTION NO: 1128

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

A.
Provide detailed instructions on how to carry out different types of tasks

B.
Ensure consistency of activities to provide a more stable environment

C.
Ensure compliance to security standards and regulatory requirements

D.
Ensure reusability to meet compliance to quality requirements

Answer: B

Explanation:

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

QUESTION NO: 1129

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

A.
Retrieve identification badge and card keys

B.
Retrieve all personal computer equipment

C.
Erase all of the employee's folders

D.
Ensure all logical access is removed

Answer: D
Explanation:

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

QUESTION NO: 1130

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.

Answer: A
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 NO: 1131

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

A.
Conduct awareness sessions on intellectual property policy

B.
Require all employees to sign a nondisclosure agreement

C.
Promptly remove all access when an employee leaves the organization

D.
Restrict access to a need-to-know basis

Answer: D

Explanation:

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

QUESTION NO: 1132

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

A.
Data owner

B.
Data custodian

C.
Systems programmer

D.
Security administrator

Answer: C
Explanation:

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

QUESTION NO: 1133

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

A.
Restrict account access to read only

B.
Log all usage of this account

C.
Suspend the account and activate only when needed

D.
Require that a change request be submitted for each download

Answer: A
Explanation:

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

QUESTION NO: 1134

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

A.
Install an antispam system

B.
Publish security guidance for customers

C.
Provide security awareness to the organization's staff

D.
Install an application-level firewall

Answer: B
Explanation:

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

QUESTION NO: 1135

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.

Answer: A
Explanation:

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

QUESTION NO: 1136

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

Answer: C
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 NO: 1137

An information security manager wishing to establish security baselines would:

A.
include appropriate measurements in the system development life cycle.

B.
implement the security baselines to establish information security best practices.

C.
implement the security baselines to fulfill laws and applicable regulations in different jurisdictions.

D.
leverage information security as a competitive advantage.

Answer: B
Explanation:

While including appropriate measurements in the system development life cycle may indicate a security baseline practice; these are wider in scope and, thus, implementing security baselines to establish information security best practices is the appropriate answer. Implementing security baselines to fulfill laws and applicable regulations in different jurisdictions, and leveraging information security as a competitive advantage may be supplementary benefits of using security baselines.

QUESTION NO: 1138

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

A.
policy.

B.
strategy.

C.
guideline

D.
baseline.

Answer: A
Explanation:

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

QUESTION NO: 1139

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

A.
references from other organizations.

B.
past experience of the engagement team.

C.
sample deliverable.

D.
methodology used in the assessment.

Answer: D
Explanation:

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

QUESTION NO: 1140

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

A.
assess the problems and institute rollback procedures, if needed.

B.
disconnect the systems from the network until the problems are corrected.

C.
immediately uninstall the patches from these systems.

D.
immediately contact the vendor regarding the problems that occurred.

Answer: A
Explanation:

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

QUESTION NO: 1141

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.

Answer: A

Explanation:

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

QUESTION NO: 1142

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.

Answer: B

Explanation:

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

QUESTION NO: 1143

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

A.

incidents may have a high impact and frequency

B.
legislation requires strong information security controls

C.
incidents may have a high impact but low frequency

D.
Electronic commerce is a primary business driver

Answer: A
Explanation:

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

QUESTION NO: 1144

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

A.
System monitoring for traffic on network ports

B.
Security code reviews for the entire application

C.
Reverse engineering the application binaries

D.
Running the application from a high-privileged account on a test system

Answer: B

Explanation:

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

QUESTION NO: 1145

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

A.
source routing.

B.
broadcast propagation.

C.
unregistered ports.

D.
nonstandard protocols.

Answer: A

Explanation:

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

QUESTION NO: 1146

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

A.
Employee monetary incentives

B.
User education and training

C.
A zero-tolerance security policy

D.
Reporting of security infractions

Answer: B
Explanation:

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

QUESTION NO: 1147

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

Answer: D
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 NO: 1148

Data owners will determine what access and authorizations users will have by:

A.
delegating authority to data custodian.

B.
cloning existing user accounts.

C.
determining hierarchical preferences.

D.
mapping to business needs.

Answer: D
Explanation:

Access and authorizations should be based on business needs. Data custodians implement the decisions made by data owners. Access and authorizations are not to be assigned by cloning existing user accounts or determining hierarchical preferences. By cloning, users may obtain more access rights and privileges than is required to do their job. Hierarchical preferences may be based on individual preferences and not on business needs.

QUESTION NO: 1149

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

Answer: A
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 NO: 1150

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

A.
Review of various security models

B.
Discussion of how to construct strong passwords

C.
Review of roles that have privileged access

D.
Discussion of vulnerability assessment results

Answer: B
Explanation:

QUESTION NO: 1151

A critical component of a continuous improvement program for information security is:

A.

measuring processes and providing feedback.

B.
developing a service level agreement (SLA) for security.

C.
tying corporate security standards to a recognized international standard.

D.
ensuring regulatory compliance.

Answer: A
Explanation:

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

QUESTION NO: 1152

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.

Answer: C
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 NO: 1153

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

A.
Rule-based

B.
Mandatory

C.
Discretionary

D.
Role-based

Answer: D

Explanation:

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

QUESTION NO: 1154

An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

A.

an audit of the service provider uncovers no significant weakness.

B.
the contract includes a nondisclosure agreement (NDA) to protect the organization's intellectual property.

C.
the contract should mandate that the service provider will comply with security policies.

D.
the third-party service provider conducts regular penetration testing.

Answer: C
Explanation:

It is critical to include the security requirements in the contract based ON the company's security policy to ensure that the necessary security controls are implemented by the service provider. The audit is normally a one-time effort and cannot provide ongoing assurance of the security. A nondisclosure agreement (NDA) should be part of the contract; however, it is not critical to the security of the web site. Penetration testing alone would not provide total security to the web site; there are lots of controls that cannot be tested through penetration testing.

QUESTION NO: 1155

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

Answer: C
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 NO: 1156

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.

Answer: A
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 NO: 1157

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

A.
Request that the third-party provider perform background checks on their employees.

B.
Perform an internal risk assessment to determine needed controls.

C.
Audit the third-party provider to evaluate their security controls.

D.
Perform a security assessment to detect security vulnerabilities.

Answer: B
Explanation:

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

QUESTION NO: 1158

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

Answer: D
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 NO: 1159

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

Answer: D
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 NO: 1160

What is the MOST cost-effective method of identifying new vendor vulnerabilities?

A.
External vulnerability reporting sources

B.
Periodic vulnerability assessments performed by consultants

C.
Intrusion prevention software

D.

honey pots located in the DMZ

Answer: A

Explanation:

External vulnerability sources are going to be the most cost-effective method of identifying these vulnerabilities. The cost involved in choices B and C would be much higher, especially if performed at regular intervals. Honeypots would not identify all vendor vulnerabilities. In addition, honeypots located in the DMZ can create a security risk if the production network is not well protected from traffic from compromised honey pots.

QUESTION NO: 1161

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

A.
Conduct periodic security audits.

B.
Perform periodic penetration testing.

C.
Define and monitor security metrics.

D.
Survey business units for feedback.

Answer: C

Explanation:

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

QUESTION NO: 1162

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

A.
validate and sanitize client side inputs.

B.
harden the database listener component.

C.
normalize the database schema to the third normal form.

D.
ensure that the security patches are updated on operating systems.

Answer: A
Explanation:

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

QUESTION NO: 1163

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

A.
uses multiple redirects for completing a data commit transaction.

B.
has implemented cookies as the sole authentication mechanism.

C.
has been installed with a non-legitimate license key.

D.
is hosted on a server along with other applications.

Answer: B
Explanation:

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

QUESTION NO: 1164

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

A.
periodic vulnerability assessment.

B.
regulatory and legal requirements.

C.
device storage capacity and longevity.

D.
past litigation.

Answer: B
Explanation:

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

QUESTION NO: 1165

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

Answer: C
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 NO: 1166

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

A.
Right to audit

B.
Nondisclosure agreement

C.
Proper firewall implementation

D.
Dedicated security manager for monitoring compliance

Answer: A

Explanation:

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a business need to examine whether the controls are working effectively at the third party. Options B, C and D are important requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

QUESTION NO: 1167

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

A.
Provide security awareness training to the third-party provider's employees

B.
Conduct regular security reviews of the third-party provider

C.
Include security requirements in the service contract

D.
Request that the third-party provider comply with the organization's information security policy

Answer: B

Explanation:

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

QUESTION NO: 1168

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.

Answer: D

Explanation:

QUESTION NO: 1169

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

Answer: D

Explanation:

QUESTION NO: 1170

Which of the following **BEST** demonstrates the maturity of an information security monitoring program?

A.
Senior management regularly reviews security standards.

B.
The information security program was introduced with a thorough business case.

C.
Information security key risk indicators (KRIs) are tied to business operations.

D.
Risk scenarios are regularly entered into a risk register.

Answer: C
Explanation:

QUESTION NO: 1171

The **PRIMARY** purpose of a security information and event management (SIEM) system is to:

A.
resolve incidents.

B.
track ongoing incidents.

C.
provide status of incidents.

D.
identify potential incidents.

Answer: D
Explanation:

QUESTION NO: 1172

Which of the following is the **STRONGEST** indication that senior management commitment to information security is lacking within an organization?

A.
A high level of information security risk acceptance

B.
The information security manager reports to the chief risk officer

C.
Inconsistent enforcement of information security policies

D.
A reduction in information security investment

Answer: C
Explanation:

QUESTION NO: 1173

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

Answer: C
Explanation:

QUESTION NO: 1174

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.

Answer: D
Explanation:

QUESTION NO: 1175

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

Answer: B
Explanation:

QUESTION NO: 1176

In a large organization, which of the following is the **BEST** source for identifying ownership of a

PC?

A.
User ID register

B.
Asset management register

C.
Domain name server (DNS) records

D.
Identity management system

Answer: B
Explanation:

QUESTION NO: 1177

The **BEST** way to obtain funding from senior management for a security awareness program is to:

A.
meet regulatory requirements.

B.
produce an impact analysis report of potential breaches.

C.
produce a report of organizational risks.

D.
demonstrate that the program will adequately reduce risk

Answer: D
Explanation:

QUESTION NO: 1178

To minimize security exposure introduced by changes to the IT environment, which of the following is **MOST** important to implement as part of change management?

A.
Requiring approval by senior management

B.
Performing a business impact analysis (BIA) prior to implementation

C.
Performing post-change reviews before closing change tickets

D.
Conducting a security risk assessment prior to go-live

Answer: B
Explanation:

QUESTION NO: 1179

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

Answer: B
Explanation:

QUESTION NO: 1180

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

Answer: D
Explanation:

QUESTION NO: 1181

Which of the following is the **BEST** way to ensure information security metrics are meaningful?

A.
Using a dashboard to present the information security metrics

B.
Requiring information security metrics to be approved by senior management

C.
Aligning information security metrics with business drivers

D.
Correlating information security metrics to industry best practices

Answer: C
Explanation:

QUESTION NO: 1182

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.

Answer: D
Explanation:

QUESTION NO: 1183

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.

Answer: A
Explanation:

QUESTION NO: 1184

Which of the following is the **MOST** effective method to help ensure information security incidents are reported?

A.

Providing information security awareness training to employees

B.

Integrating information security language in conditions of employment

C.

Integrating information security language in corporate compliance rules

D.

Implementing an incident management system

Answer: A

Explanation:

QUESTION NO: 1185

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

Answer: B

Explanation:

QUESTION NO: 1186

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.

Answer: B
Explanation:

QUESTION NO: 1187

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

Answer: A
Explanation:

QUESTION NO: 1188

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

Answer: A

Explanation:

QUESTION NO: 1189

Which of the following processes would BEST aid an information security manager in resolving systemic security issues?

A.
Root cause analysis

B.
Business impact analysis (BIA)

C.
Reinforced security controls

D.
Security reviews

Answer: A

Explanation:

QUESTION NO: 1190

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.

Answer: D
Explanation:

QUESTION NO: 1191

Which of the following features of a library control software package would protect against unauthorized updating of source code?

A.
Required approvals at each life cycle step

B.
Date and time stamping of source and object code

C.
Access controls for source libraries

D.
Release-to-release comparison of source code

Answer: C
Explanation:

QUESTION NO: 1192

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.

Answer: C
Explanation:

QUESTION NO: 1193

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.

Answer: B
Explanation:

QUESTION NO: 1194

The **PRIMARY** goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A.
map the business process to supporting IT and other corporate resources.

B.
obtain the support of executive management.

C.
document the disaster recovery process.

D.
identify critical processes and the degree of reliance on support services.

Answer: D
Explanation:

QUESTION NO: 1195

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).

Answer: A
Explanation:

QUESTION NO: 1196

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

Answer: D
Explanation:

QUESTION NO: 1197

What should an information security team do **FIRST** when notified by the help desk that an employee's computer has been infected with malware?

A.
Take a forensic copy of the hard drive.

B.
Restore the files from a secure backup.

C.
Isolate the computer from the network.

D.
Use anti-malware software to clean the infected computer.

Answer: C
Explanation:

QUESTION NO: 1198

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.

Answer: B
Explanation:

QUESTION NO: 1199

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.

Answer: A
Explanation:

QUESTION NO: 1200

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

Answer: C
Explanation:

QUESTION NO: 1201

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

Answer: B
Explanation:

QUESTION NO: 1202

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)

Answer: D
Explanation:

QUESTION NO: 1203

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

Answer: C
Explanation:

QUESTION NO: 1204

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

Answer: D
Explanation:

QUESTION NO: 1205

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

Answer: C
Explanation:

QUESTION NO: 1206

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

Answer: A
Explanation:

QUESTION NO: 1207

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.

Answer: A
Explanation:

QUESTION NO: 1208

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.

Answer: A
Explanation:

QUESTION NO: 1209

Which of the following is the **MOST** effective approach to communicate general information security responsibilities across an organization?

A.
Require staff to sign confidentiality agreements.

B.
Develop a RACI matrix for the organization.

C.
Specify information security responsibilities in job descriptions.

D.
Provide regular security awareness training.

Answer: C
Explanation:

QUESTION NO: 1210

The **MOST** important reason for an information security manager to be involved in a new software purchase initiative is to:

A.
choose the software with the most control options.

B.
provide input for user requirements.

C.
ensure there is software escrow in place.

D.
ensure the appropriate controls are considered.

Answer: D
Explanation:

QUESTION NO: 1211

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.

Answer: C
Explanation:

QUESTION NO: 1212

Which of the following is the **MOST** reliable source of information about emerging information security threats and vulnerabilities?

A.
Industry bloggers

B.
A social media group of hackers

C.
Threat intelligence groups

D.
Vulnerability scanning alerts

Answer: C
Explanation:

QUESTION NO: 1213

An organization is about to purchase a rival organization. The **PRIMARY** reason for performing information security due diligence prior to making the purchase is to:

A.
ensure compliance with international standards.

B.
assess the ability to integrate the security department operations.

C.
determine the security exposures.

D.
evaluate the security policy and standards.

Answer: C
Explanation:

QUESTION NO: 1214

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

Answer: D

Explanation:

QUESTION NO: 1215

Which of the following is **MOST** helpful for protecting an enterprise from advanced persistent threats (APTs)?

A.
Defined security standards

B.
Updated security policies

C.
Threat intelligence

D.
Regular antivirus updates

Answer: C

Explanation:

QUESTION NO: 1216

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

Answer: A
Explanation:

QUESTION NO: 1217

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.

Answer: B
Explanation:

QUESTION NO: 1218

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

Answer: A
Explanation:

QUESTION NO: 1219

What is the **MOST** important role of an organization's data custodian in support of the information security function?

A.
Evaluating data security technology vendors

B.
Assessing data security risks to the organization

C.
Approving access rights to departmental data

D.
Applying approved security policies

Answer: D
Explanation:

QUESTION NO: 1220

Which of the following is **MOST** relevant for an information security manager to communicate to business units?

A.
Threat assessments

B.
Vulnerability assessments

C.
Risk ownership

D.
Business impact analysis (BIA)

Answer: D
Explanation:

QUESTION NO: 1221

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

Answer: C
Explanation:

QUESTION NO: 1222

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

Answer: A
Explanation:

QUESTION NO: 1223

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

Answer: C
Explanation:

QUESTION NO: 1224

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

Answer: A
Explanation:

QUESTION NO: 1225

Which of the following should cause the **GREATEST** concern for an information security manager reviewing the effectiveness of an intrusion prevention system (IPS)?

A.
Increase in false negatives

B.
Decrease in malicious packets

C.
Decrease in false positives

D.
Increase in crossover error rate

Answer: A
Explanation:

QUESTION NO: 1226

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

Answer: D

Explanation:

QUESTION NO: 1227

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.

Answer: A

Explanation:

QUESTION NO: 1228

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.

Answer: B
Explanation:

QUESTION NO: 1229

Penetration testing is **MOST** appropriate when a:

A.
new system is about to go live.

B.
security incident has occurred.

C.
security policy is being developed.

D.
new system is being designed.

Answer: A
Explanation:

QUESTION NO: 1230

Which of the following should be the **FIRST** step to ensure system updates are applied in a timely manner?

A.
Run a patch management scan to discover which patches are missing from each machine.

B.
Create a regression test plan to ensure business operation is not interrupted.

C.
Cross-reference all missing patches to establish the date each patch was introduced.

D.
Establish a risk-based assessment process for prioritizing patch implementation.

Answer: A
Explanation:

QUESTION NO: 1231

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

A.
Design a training program for the staff involved to heighten information security awareness

B.
Set role-based access permissions on the shared folder

C.
The end user develops a PC macro program to compare sender and recipient file contents

D.
Shared folder operators sign an agreement to pledge not to commit fraudulent activities

Answer: B
Explanation:

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

QUESTION NO: 1232

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

A.
A problem management process

B.
Background screening

C.
A change control process

D.
Business impact analysis (BIA)

Answer: C
Explanation:

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

QUESTION NO: 1233

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

A.
Vulnerability scans

B.
Penetration tests

C.
Code reviews

D.
Security audits

Answer: B
Explanation:

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

QUESTION NO: 1234

In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

A.
Procedural design

B.
Architectural design

C.
System design specifications

D.
Software development

Answer: C

Explanation:

The system design specifications phase is when security specifications are identified. The procedural design converts structural components into a procedural description of the software. The architectural design is the phase that identifies the overall system design, hut not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.

QUESTION NO: 1235

Which of the following is generally considered a fundamental component of an information security program?

A.
Role-based access control systems

B.
Automated access provisioning

C.
Security awareness training

D.
Intrusion prevention systems (IPSs)

Answer: C

Explanation:

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

QUESTION NO: 1236

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.

Answer: A
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 NO: 1237

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.

Answer: C
Explanation:

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

QUESTION NO: 1238

Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A.
Acceptable use policy

B.
Setting low mailbox limits

C.
User awareness training

D.
Taking disciplinary action

Answer: C
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 NO: 1239

Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

A.
Passwords stored in encrypted form

B.
User awareness

C.
Strong passwords that are changed periodically

D.
Implementation of lock-out policies

Answer: D
Explanation:

Implementation of account lock-out policies significantly inhibits brute-force attacks. In cases where this is not possible, strong passwords that are changed periodically would be an appropriate choice. Passwords stored in encrypted form will not defeat an online brute-force attack if the password itself is easily guessed. User awareness would help but is not the best approach of the options given.

QUESTION NO: 1240

Which of the following measures is the MOST effective deterrent against disgruntled stall abusing their privileges?

A.
Layered defense strategy

B.
System audit log monitoring

C.
Signed acceptable use policy

D.
High-availability systems

Answer: C
Explanation:

A layered defense strategy would only prevent those activities that are outside of the user's privileges. A signed acceptable use policy is often an effective deterrent against malicious activities because of the potential for termination of employment and/or legal actions being taken against the individual. System audit log monitoring is after the fact and may not be effective. High-availability systems have high costs and are not always feasible for all devices and components or systems.

QUESTION NO: 1241

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.

Answer: A
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 NO: 1242

As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A.
considered at the discretion of the information owner.

B.
approved by the next higher person in the organizational structure.

C.
formally managed within the information security framework.

D.
reviewed and approved by the security manager.

Answer: C
Explanation:

A formal process for managing exceptions to information security policies and standards should be included as part of the information security framework. The other options may be contributors to the process but do not in themselves constitute a formal process.

QUESTION NO: 1243

There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

A.
Black box pen test

B.
Security audit

C.
Source code review

D.
Vulnerability scan

Answer: C
Explanation:

Source code review is the best way to find and remove an application backdoor. Application backdoors can be almost impossible to identify' using a black box pen test or a security audit. A vulnerability scan will only find "known" vulnerability patterns and will therefore not find a programmer's application backdoor.

QUESTION NO: 1244

Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does it always introduce?

A.
Remote buffer overflow

B.
Cross site scripting

C.
Clear text authentication

D.
Man-in-the-middle attack

Answer: C
Explanation:

One of the main problems with using SNMP vl and v°2 is the clear text "community string" that it uses to authenticate. It is easy to sniff and reuse. Most times, the SNMP community string is shared throughout the organization's servers and routers, making this authentication problem a serious threat to security. There have been some isolated cases of remote buffer overflows against SNMP daemons, but generally that is not a problem. Cross site scripting is a web application vulnerability that is not related to SNMP. A man-in-the-middle attack against a user datagram protocol (UDP) makes no sense since there is no active session; every request has the community string and is answered independently.

QUESTION NO: 1245

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

Answer: D
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 NO: 1246

Which of the following is the MOST important consideration when deciding whether to continue outsourcing to a managed security service provider?

A.
The business need for the function

B.
The cost of the services

C.
The vendor’s reputation in the industry

D.
The ability to meet deliverables

Answer: D
Explanation:

QUESTION NO: 1247

Which of the following BEST ensures timely and reliable access to services?

A.
Authenticity

B.
Recovery time objective

C.
Availability

D.
Nonrepudiation

Answer: C
Reference: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

QUESTION NO: 1248

Which of the following would be **MOST** effective in ensuring that information security is appropriately addressed in new systems?

A.
Internal audit signs off on security prior to implementation

B.
Information security staff perform compliance reviews before production begins

C.
Information security staff take responsibility for the design of system security

D.
Business requirements must include security objectives

Answer: D
Explanation:

QUESTION NO: 1249

An information security manager learns that a departmental system is out of compliance with the information security policy's password strength requirements. Which of the following should be the information security manager's FIRST course of action?

A.

Submit the issue to the steering committee for escalation

B.
Conduct an impact analysis to quantify the associated risk

C.
Isolate the non-compliant system from the rest of the network

D.
Request risk acceptance from senior management

Answer: C
Explanation:

QUESTION NO: 1250

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

Answer: C
Explanation:

QUESTION NO: 1251

Attacks using multiple methods to spread should be classified:

A.
each time the exposure is experienced

B.

depending on the method used to spread

C.

at the highest potential level of business impact

D.

using multiple classifications for each impact

Answer: C

Explanation:

QUESTION NO: 1252

A semi-annual disaster recovery test has been completed. Which of the following issues discussed during the lessons learned phase should be of GREATEST concern?

A.

A server used in recovery did not have the latest security patches

B.

Application testing was completed by system administrators

C.

Poor network performance was reported during recovery

D.

Some restored systems were not listed in the DNS table of the DR subnet

Answer: C

Explanation:

QUESTION NO: 1253

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

Answer: C
Explanation:

QUESTION NO: 1254

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

Answer: B
Explanation:

QUESTION NO: 1255

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

Answer: A
Explanation:

QUESTION NO: 1256

Which of the following will protect the confidentiality of data transmitted over the Internet?

A.
Message digests

B.
Network address translation

C.
Encrypting file system

D.
IPsec protocol

Answer: D
Explanation:

QUESTION NO: 1257

The business advantage of implementing authentication tokens is that they:

A.
provide nonrepudiation

B.
reduce overall cost

C.
improve access security

D.
reduce administrative workload

Answer: C
Explanation:

QUESTION NO: 1258

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

Answer: D
Explanation:

QUESTION NO: 1259

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

Answer: C
Explanation:

QUESTION NO: 1260

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)

Answer: D
Explanation:

QUESTION NO: 1261

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

Answer: C
Explanation:

QUESTION NO: 1262

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

Answer: B
Explanation:

QUESTION NO: 1263

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)

Answer: C

Explanation:

QUESTION NO: 1264

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

Answer: D

Explanation:

QUESTION NO: 1265

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

Answer: A
Explanation:

QUESTION NO: 1266

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.

Answer: A
Explanation:

QUESTION NO: 1267

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).

Answer: D

Explanation:

QUESTION NO: 1268

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.

Answer: B

Explanation:

QUESTION NO: 1269

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

Answer: A

Explanation:

QUESTION NO: 1270

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.

Answer: D

Explanation:

QUESTION NO: 1271

Which of the following is the **GREATEST** security concern when an organization allows the use of social networks?

A.
Network performance degradation

B.
Browser vulnerability exploitation

C.
Decreased user productivity

D.

Inadvertent data disclosure

Answer: D

Explanation:

QUESTION NO: 1272

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.

Answer: B

Explanation:

QUESTION NO: 1273

Which of the following is the **MOST** important reason to have documented security procedures and guidelines?

A.
To meet regulatory compliance requirements

B.
To allocate security responsibilities to staff

C.
To facilitate collection of security metrics

D.
To enable standard security practices

Answer: A

Explanation:

QUESTION NO: 1274

Which of the following recovery approaches generally has the **LOWEST** periodic cost?

A.
Redundant site

B.
Reciprocal agreement

C.
Shared contingency center

D.
Cold site

Answer: D

Explanation:

QUESTION NO: 1275

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

Answer: B

Explanation:

QUESTION NO: 1276

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.

Answer: C

Explanation:

QUESTION NO: 1277

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

Answer: D

Explanation:

QUESTION NO: 1278

Which of the following is the **MOST** effective way for an information security manager to protect the organization from misuse of social media?

A.
Hire a social media manager to control content delivered via social media.

B.
Scan social media platforms for company references.

C.
Restrict the use of social media on corporate networks and devices.

D.
Deliver regular social media awareness training to all employees.

Answer: C
Explanation:

QUESTION NO: 1279

Which of the following is the **GREATEST** benefit of a centralized approach to coordinating information security?

A.
Optimal use of security resources

B.
Reduction in the number of policies

C.
Business user buy-in

D.
Integration with business functions

Answer: A

Explanation:

QUESTION NO: 1280

Which of the following factors is **MOST** likely to increase the chances of a successful social engineering attack?

A.
Technical skills.

B.
Knowledge of internal procedures

C.
Potential financial gain

D.
Weak authentication for remote access

Answer: B
Explanation:

QUESTION NO: 1281

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

Answer: B

Explanation:

QUESTION NO: 1282

Which of the following presents the **GREATEST** concern to the information security manager when using account locking features on an online application? It can increase vulnerability to:

A.
brute force attacks

B.
social engineering

C.
denial of service

D.
phishing

Answer: C

Explanation:

QUESTION NO: 1283

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.

Answer: C

Explanation:

QUESTION NO: 1284

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

Answer: A

Explanation:

QUESTION NO: 1285

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.

Answer: A

Explanation:

Topic 5, INCIDENT MANAGEMENT AND RESPONSE

QUESTION NO: 1286

An attacker was able to gain access to an organization's perimeter firewall and made changes to allow wider external access and to steal data. Which of the following would have **BEST** provided timely identification of this incident?

A.
Deploying a security information and event management system (SIEM)

B.
Deploying an intrusion prevention system (IPS)

C.
Implementing a data loss prevention (DLP) suite

D.
Conducting regular system administrator awareness training

Answer: A

Explanation:

QUESTION NO: 1287

An organization finds unauthorized software has been installed on a number of workstations. The software was found to contain a Trojan which had been uploading data to an unknown external party. Which of the following would have **BEST** prevented the installation of the unauthorized software?

A.
Implementing application blacklisting

B.
Implementing an intrusion detection system (IDS)

C.
Banning executable file downloads at the Internet firewall

D.
Removing local administrator rights

Answer: D
Explanation:

QUESTION NO: 1288

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.

Answer: A
Explanation:

QUESTION NO: 1289

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.

Answer: D

Explanation:

QUESTION NO: 1290

When a business-critical web server is compromised, the IT security department should **FIRST**:

A.
archive the logs as evidence.

B.
attempt to repair any damage in order to keep the server running.

C.
notify the legal department and/or regulatory officials as required.

D.
advise management of the incident.

Answer: D

Explanation:

QUESTION NO: 1291

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.

Answer: C
Explanation:

QUESTION NO: 1292

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

Answer: D
Explanation:

QUESTION NO: 1293

Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will **BEST** enable a cloud service provider to assist customers when recovering from a security incident?

A.
Availability of current infrastructure documentation

B.

Capability to take a snapshot of virtual machines

C.

Availability of web application firewall logs

D.

Capability of online virtual machine analysis

Answer: B

Explanation:

QUESTION NO: 1294

Which of the following is the **BEST** reason to reassess risk following an incident?

A.

To capture lessons learned

B.

To identify changes in the threat environment

C.

To update roles and responsibilities

D.

To accurately document risk to the organization

Answer: D

Explanation:

QUESTION NO: 1295

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.

Answer: D
Explanation:

QUESTION NO: 1296

Which of the following would provide the **MOST** comprehensive view of the effectiveness of the information security function within an organization?

A.
An incident reporting system

B.
Examples of compliance with security processes

C.
A balanced scorecard

D.
An interview with senior managers

Answer: A
Explanation:

QUESTION NO: 1297

When developing an incident response plan, which of the following is the **MOST** effective way to ensure incidents common to the organization are handled properly?

A.
Adopting industry standard response procedures

B.
Rehearsing response scenarios

C.
Conducting awareness training

D.
Creating and distributing a personnel call tree

Answer: A
Explanation:

QUESTION NO: 1298

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.

Answer: D
Explanation:

QUESTION NO: 1299

Which of the following is **MOST** important when prioritizing an information security incident?

A.
Organizational risk tolerance

B.

Cost to contain and remediate the incident

C.
Critically of affected resources

D.
Short-term impact to shareholder value

Answer: C
Explanation:

QUESTION NO: 1300

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

Answer: D
Explanation:

QUESTION NO: 1301

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

Answer: A
Explanation:

QUESTION NO: 1302

During an emergency security incident, which of the following would **MOST** likely predict the worst-case scenario?

A.
Cost-benefit analysis report

B.
Business impact analysis (BIA) report

C.
Risk assessment report

D.
Vulnerability assessment report

Answer: C
Explanation:

QUESTION NO: 1303

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

Answer: B
Explanation:

QUESTION NO: 1304

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.

Answer: C
Explanation:

QUESTION NO: 1305

Which of the following provides the **MOST** relevant evidence of incident response maturity?

A.
Red team testing results

B.
Average incident closure time

C.
Independent audit assessment

D.
Tabletop exercise results

Answer: C

Explanation:

QUESTION NO: 1306

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

Answer: B

Explanation:

QUESTION NO: 1307

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.

Answer: A
Explanation:

QUESTION NO: 1308

Which of the following is the **PRIMARY** objective of an incident communication plan?

A.
To convey information about the incident to those affected by it

B.
To prevent reputational damage to the organization

C.
To prevent unannounced visits from the media during crisis

D.
To fulfill regulatory requirements for incident response

Answer: A
Explanation:

QUESTION NO: 1309

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

Answer: A

Explanation:

QUESTION NO: 1310

Which of the following should be the PRIMARY objective of the information security incident response process?

A.

Conducting incident triage

B.

Classifying incidents

C.

Communicating with internal and external parties

D.

Minimizing negative impact to critical operations

Answer: D

Explanation:

QUESTION NO: 1311

Which of the following is the PRIMARY purpose of red team testing?

A.

To determine the organization’s preparedness for an attack

B.

To assess the vulnerability of employees to social engineering

C.

To establish a baseline incident response program

D.

To confirm the risk profile of the organization

Answer: A

Explanation:

QUESTION NO: 1312

Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

A.
Recognized threat intelligence communities

B.
Open-source reconnaissance

C.
Disaster recovery consultants widely endorsed in industry forums

D.
Incident response experts from highly regarded peer organizations

Answer: D

Explanation:

QUESTION NO: 1313

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

Answer: A

Explanation:

QUESTION NO: 1314

Which of the following is the MOST important reason for logging firewall activity?

A.
Incident investigation

B.
Auditing purposes

C.
Intrusion detection

D.
Firewall tuning

Answer: A

Explanation:

QUESTION NO: 1315

Which of the following is the BEST way to improve the timely reporting of information security incidents?

A.
Perform periodic simulations with the incident response team

B.
Integrate an intrusion detection system (IDS) in the DMZ

C.
Incorporate security procedures in help desk processes

D.
Regularly reassess and update the incident response plan

Answer: B

Explanation:

QUESTION NO: 1316

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

Answer: C

Explanation:

QUESTION NO: 1317

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

A.
Post-incident analysis results

B.
The risk management process

C.
The security awareness programs

D.
Firewall logs

Answer: B

Explanation:

QUESTION NO: 1318

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

Answer: D

Explanation:

QUESTION NO: 1319

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

Answer: C

Explanation:

QUESTION NO: 1320

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

Answer: C

Explanation:

QUESTION NO: 1321

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

Answer: B

Explanation:

QUESTION NO: 1322

Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

A.
Identify unmitigated risk

B.
Prevent incident recurrence

C.
Evaluate the security posture of the organization

D.
Support business investments in security

Answer: B

Explanation:

QUESTION NO: 1323

Which of the following is the MOST important part of an incident response plan?

A.
Recovery time objective (RTO)

B.
Business impact analysis (BIA)

C.
Recovery point objective (RPO)

D.
Mean time to report (MTTR)

Answer: A

Explanation:

QUESTION NO: 1324

When designing an incident response plan to be agreed upon with a cloud computing vendor, including which of the following will BEST help to ensure the effectiveness of the plan?

A.
A training program for the vendor staff

B.
An audit and compliance program

C.
Responsibility and accountability assignments

D.
Requirements for onsite recovery testing

Answer: C
Explanation:

QUESTION NO: 1325

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

Answer: B

Explanation:

QUESTION NO: 1326

Following a highly sensitive data breach at a large company, all servers and workstations were patched. The information security manager’s **NEXT** step should be to:

A.
inform senior management of changes in risk metrics.

B.
perform an assessment to measure the current state.

C.
deliver security awareness training.

D.
ensure baseline back-ups are performed.

Answer: B

Explanation:

QUESTION NO: 1327

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.

Answer: A

Explanation:

QUESTION NO: 1328

Which of the following should be determined FIRST when establishing a business continuity program?

A.
Cost to rebuild information processing facilities

B.
Incremental daily cost of the unavailability of systems

C.
Location and cost of offsite recovery facilities

D.
Composition and mission of individual recovery teams

Answer: B

Explanation:

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION NO: 1329

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.

Answer: A
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 NO: 1330

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

Answer: D
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 NO: 1331

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

Answer: C
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 NO: 1332

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.

Answer: C
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 NO: 1333

The FIRST priority when responding to a major security incident is:

A.
documentation.

B.
monitoring.

C.
restoration.

D.
containment.

Answer: D
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 NO: 1334

Which of the following is the MOST important to ensure a successful recovery?

A.
Backup media is stored offsite

B.
Recovery location is secure and accessible

C.
More than one hot site is available

D.
Network alternate links are regularly tested

Answer: A
Explanation:

Unless backup media are available, all other preparations become meaningless. Recovery site location and security are important, but would not prevent recovery in a disaster situation. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, alternate data communication lines should be tested regularly and successfully but, again, this is not as critical.

QUESTION NO: 1335

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

Answer: D
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 NO: 1336

At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

A.
Erase data and software from devices

B.
Conduct a meeting to evaluate the test

C.
Complete an assessment of the hot site provider

D.
Evaluate the results from all test scripts

Answer: A
Explanation:

For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations can occur back at the office after everyone is rested, and the overall results can be discussed and compared objectively.

QUESTION NO: 1337

An incident response policy must contain:

A.
updated call trees.

B.
escalation criteria.

C.
press release templates.

D.
critical backup files inventory.

Answer: B
Explanation:

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

QUESTION NO: 1338

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.

Answer: A
Explanation:

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

QUESTION NO: 1339

A post-incident review should be conducted by an incident management team to determine:

A.
relevant electronic evidence.

B.
lessons learned.

C.
hacker's identity.

D.
areas affected.

Answer: B
Explanation:

Post-incident reviews are beneficial in determining ways to improve the response process through lessons learned from the attack. Evaluating the relevance of evidence, who launched the attack or what areas were affected are not the primary purposes for such a meeting because these should have been already established during the response to the incident.

QUESTION NO: 1340

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

A.
communication line capacity between data centers.

B.
current processing capacity loads at data centers.

C.

differences in logical security at each center.

D.
synchronization of system software release versions.

Answer: B
Explanation:

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

QUESTION NO: 1341

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

A.
Only business data files from offsite storage are used

B.
IT staff fully recovers the processing infrastructure

C.
Critical business processes are duplicated

D.
All systems are restored within recovery time objectives (RTOs)

Answer: C
Explanation:

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

QUESTION NO: 1342

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

A.
Cost to build a redundant processing facility and invocation

B.
Daily cost of losing critical systems and recovery time objectives (RTOs)

C.
Infrastructure complexity and system sensitivity

D.
Criticality results from the business impact analysis (BIA)

Answer: C
Explanation:

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

QUESTION NO: 1343

A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

A.

Quarantine all picture files stored on file servers

B.
Block all e-mails containing picture file attachments

C.
Quarantine all mail servers connected to the Internet

D.
Block incoming Internet mail, but permit outgoing mail

Answer: B
Explanation:

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

QUESTION NO: 1344

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

Answer: C
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 NO: 1345

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

A.
A hot site facility will be shared in multiple disaster declarations

B.
All equipment is provided "at time of disaster, not on floor"

C.
The facility is subject to a "first-come, first-served" policy

D.
Equipment may be substituted with equivalent model

Answer: B
Explanation:

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

QUESTION NO: 1346

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

A.
Restore servers from backup media stored offsite

B.

Conduct an assessment to determine system status

C.
Perform an impact analysis of the outage

D.
Isolate the screened subnet

Answer: B
Explanation:

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

QUESTION NO: 1347

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

A.
Detailed technical recovery plans are maintained offsite

B.
Network redundancy is maintained through separate providers

C.
Hot site equipment needs are recertified on a regular basis

D.
Appropriate declaration criteria have been established

Answer: A
Explanation:

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

QUESTION NO: 1348

The business continuity policy should contain which of the following?

A.
Emergency call trees

B.
Recovery criteria

C.
Business impact assessment (BIA)

D.
Critical backups inventory

Answer: B
Explanation:

Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

QUESTION NO: 1349

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

A.
weaknesses in network security.

B.
patterns of suspicious access.

C.
how an attack was launched on the network.

D.
potential attacks on the internal network.

Answer: D
Explanation:

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

QUESTION NO: 1350

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

Answer: A
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 NO: 1351

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

A.
Verify the date that signature files were last pushed out

B.
Use a recently identified benign virus to test if it is quarantined

C.
Research the most recent signature file and compare to the console

D.
Check a sample of servers that the signature files are current

Answer: D

Explanation:

The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that 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 NO: 1352

Which of the following actions should be taken when an information security manager discovers that a hacker is foot printing the network perimeter?

A.
Reboot the border router connected to the firewall

B.
Check IDS logs and monitor for any active attacks

C.
Update IDS software to the latest available version

D.
Enable server trace logging on the DMZ segment

Answer: B

Explanation:

Information security should check the intrusion detection system (IDS) logs and continue to monitor the situation. It would be inappropriate to take any action beyond that. In fact, updating the IDS could create a temporary exposure until the new version can be properly tuned. Rebooting the router and enabling server trace routing would not be warranted.

QUESTION NO: 1353

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

Answer: D
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 NO: 1354

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

A.
Most new viruses* signatures are identified over weekends

B.
Technical personnel are not available to support the operation

C.
Systems are vulnerable to new viruses during the intervening week

D.
The update's success or failure is not known until Monday

Answer: C
Explanation:

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

QUESTION NO: 1355

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

Answer: C
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 NO: 1356

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

A.
Confirming that detailed technical recovery plans exist

B.
Periodically testing network redundancy

C.
Updating the hot site equipment configuration every quarter

D.
Developing recovery time objectives (RTOs) for critical functions

Answer: D
Explanation:

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

QUESTION NO: 1357

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

Answer: C

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 NO: 1358

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

A.
Risk assessment results

B.
Severity criteria

C.
Emergency call tree directory

D.
Table of critical backup files

Answer: B

Explanation:

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

QUESTION NO: 1359

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

A.

weaknesses in network and server security.

B.
ways to improve the incident response process.

C.
potential attack vectors on the network perimeter.

D.
the optimum response to internal hacker attacks.

Answer: A
Explanation:

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

QUESTION NO: 1360

Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

A.
removed into the custody of law enforcement investigators.

B.
kept in the tape library' pending further analysis.

C.
sealed in a signed envelope and locked in a safe under dual control.

D.
handed over to authorized independent investigators.

Answer: B
Explanation:

Since a number of individuals would have access to the tape library, and could have accessed and tampered with the tape, the chain of custody could not be verified. All other choices provide clear indication of who was in custody of the tape at all times.

QUESTION NO: 1361

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

A.
Business continuity plan

B.
Disaster recovery plan

C.
Incident response plan

D.
Vulnerability management plan

Answer: C
Explanation:

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

QUESTION NO: 1362

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

Answer: C
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 NO: 1363

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

Answer: A
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 NO: 1364

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

A.
Adjust budget provisioning

B.
Preserve forensic data

C.
Improve the response process

D.
Ensure the incident is fully documented

Answer: C
Explanation:

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

QUESTION NO: 1365

Detailed business continuity plans should be based PRIMARILY on:

A.
consideration of different alternatives.

B.
the solution that is least expensive.

C.
strategies that cover all applications.

D.

strategies validated by senior management.

Answer: D

Explanation:

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

QUESTION NO: 1366

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.

Answer: D

Explanation:

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

QUESTION NO: 1367

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

Answer: A
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 NO: 1368

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.

Answer: B
Explanation:

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

QUESTION NO: 1369

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.

Answer: D
Explanation:

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

QUESTION NO: 1370

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

A.
Evaluate the impact of the information loss

B.
Update the corporate laptop inventory

C.
Ensure compliance with reporting procedures

D.
Disable the user account immediately

Answer: C
Explanation:

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

QUESTION NO: 1371

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

Answer: A
Explanation:

Before performing analysis of impact, resolution, notification or isolation of an incident, it must be validated as a real security incident.

QUESTION NO: 1372

When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

A.
services delivery objective.

B.
recovery time objective (RTO).

C.
recovery window.

D.
maximum tolerable outage (MTO).

Answer: C
Explanation:

The length of the recovery window is defined by business management and determines the acceptable time frame between a disaster and the restoration of critical services/applications. The technical implementation of the disaster recovery (DR) site will be based on this constraint, especially the choice between a hot, warm or cold site. The service delivery objective is supported during the alternate process mode until the normal situation is restored, which is directly related to business needs. The recovery time objective (RTO) is commonly agreed to be the time frame between a disaster and the return to normal operations. It is then longer than the interruption window and is very difficult to estimate in advance. The time frame between the reduced operation mode at the end of the interruption window and the return to normal operations depends on the magnitude of the disaster. Technical disaster recovery solutions alone will not be used for returning to normal operations. Maximum tolerable outage (MTO) is the maximum time acceptable by a company operating in reduced mode before experiencing losses. Theoretically, recovery time objectives (RTOs) equal the interruption window plus the maximum tolerable outage. This will not be the primary factor for the choice of the technical disaster recovery solution.

QUESTION NO: 1373

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.

Answer: B
Explanation:

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

QUESTION NO: 1374

An intrusion detection system (IDS) should:

A.

run continuously

B.
ignore anomalies

C.
require a stable, rarely changed environment

D.
be located on the network

Answer: A
Explanation:

If an intrusion detection system (IDS) does not run continuously the business remains vulnerable. An IDS should detect, not ignore anomalies. An IDS should be flexible enough to cope with a changing environment. Both host and network based IDS are recommended for adequate detection.

QUESTION NO: 1375

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.

Answer: A
Explanation:

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

QUESTION NO: 1376

Which of the following provides the BKST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

A.
The recovery time objective (RTO) was not exceeded during testing

B.
Objective testing of the business continuity/disaster recovery plan has been carried out consistently

C.
The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing

D.
Information assets have been valued and assigned to owners per the business continuity plan, disaster recovery plan

Answer: A
Explanation:

Consistent achievement of recovery time objective (RTO) objectives during testing provides the most objective evidence that business continuity/disaster recovery plan objectives have been achieved. The successful testing of the business continuity/disaster recover) plan within the stated RTO objectives is the most indicative evidence that the business needs are being met. Objective testing of the business continuity/ disaster recovery plan will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning. Mere valuation and assignment of information assets to owners (per the business continuity/disaster recovery plan) will not serve as a basis for evaluating the alignment of the risk management process in business continuity/disaster recovery planning.

QUESTION NO: 1377

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

Answer: D
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 NO: 1378

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.

Answer: A
Explanation:

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

QUESTION NO: 1379

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.

Answer: C
Explanation:

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

QUESTION NO: 1380

When collecting evidence for forensic analysis, it is important to:

A.
ensure the assignment of qualified personnel.

B.
request the IT department do an image copy.

C.
disconnect from the network and isolate the affected devices.

D.
ensure law enforcement personnel are present before the forensic analysis commences.

Answer: A

Explanation:

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

QUESTION NO: 1381

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

Answer: B

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 NO: 1382

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

Answer: D
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 NO: 1383

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

A.
Invalid logon attempts

B.
Write access violations

C.
Concurrent logons

D.
Firewall logs

Answer: A
Explanation:

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

QUESTION NO: 1384

Which of the following is an example of a corrective control?

A.
Diverting incoming traffic upon responding to the denial of service (DoS) attack

B.
Filtering network traffic before entering an internal network from outside

C.
Examining inbound network traffic for viruses

D.
Logging inbound network traffic

Answer: A
Explanation:

Diverting incoming traffic corrects the situation and, therefore, is a corrective control. Choice B is a preventive control. Choices C and D are detective controls.

QUESTION NO: 1385

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

Answer: C
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 NO: 1386

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).

Answer: D
Explanation:

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

QUESTION NO: 1387

A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

A.
Ensure that all OS patches are up-to-date

B.
Block inbound traffic until a suitable solution is found

C.
Obtain guidance from the firewall manufacturer

D.
Commission a penetration test

Answer: C
Explanation:

The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring dial all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

QUESTION NO: 1388

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.

Answer: B
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 NO: 1389

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

Answer: A
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 madetranslating business prioritization to IT prioritization. Business process mapping does not help in making a decision, but in implementing a decision.

QUESTION NO: 1390

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

Answer: B
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 NO: 1391

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.

Answer: A
Explanation:

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

QUESTION NO: 1392

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

A.
Communicating specially drafted messages by an authorized person

B.
Refusing to comment until recovery

C.
Referring the media to the authorities

D.
Reporting the losses and recovery strategy to the media

Answer: A
Explanation:

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

QUESTION NO: 1393

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.

Answer: C
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 NO: 1394

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A.
obtaining evidence as soon as possible.

B.
preserving the integrity of the evidence.

C.
disconnecting all IT equipment involved.

D.
reconstructing the sequence of events.

Answer: B
Explanation:

The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are pan of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

QUESTION NO: 1395

Which of the following has the highest priority when defining an emergency response plan?

A.
Critical data

B.
Critical infrastructure

C.
Safety of personnel

D.
Vital records

Answer: C
Explanation:

The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

QUESTION NO: 1396

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.

Answer: A
Explanation:

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

QUESTION NO: 1397

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.

Answer: A

Explanation:

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

QUESTION NO: 1398

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

A.
Incident response metrics

B.
Periodic auditing of the incident response process

C.
Action recording and review

D.
Post incident review

Answer: D

Explanation:

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

QUESTION NO: 1399

The FIRST step in an incident response plan is to:

A.

notify- the appropriate individuals.

B.
contain the effects of the incident to limit damage.

C.
develop response strategies for systematic attacks.

D.
validate the incident.

Answer: D
Explanation:

Appropriate people need to be notified; however, one must first validate the incident. Containing the effects of the incident would be completed after validating the incident. Developing response strategies for systematic attacks should have already been developed prior to the occurrence of an incident.

QUESTION NO: 1400

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

A.
Inform senior management.

B.
Determine the extent of the compromise.

C.
Report the incident to the authorities.

D.
Communicate with the affected customers.

Answer: B
Explanation:

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

QUESTION NO: 1401

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

A.
Run a port scan on the system

B.
Disable the logon ID

C.
Investigate the system logs

D.
Validate the incident

Answer: D
Explanation:

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

QUESTION NO: 1402

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.

Answer: B

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 NO: 1403

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.

Answer: B

Explanation:

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

QUESTION NO: 1404

An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

A.

Unsure that critical data on the server are backed up.

B.
Shut down the compromised server.

C.
Initiate the incident response process.

D.
Shut down the network.

Answer: C
Explanation:

The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

QUESTION NO: 1405

An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

A.
Shut down and power off the server.

B.
Duplicate the hard disk of the server immediately.

C.
Isolate the server from the network.

D.
Copy the database log file to a protected server.

Answer: C
Explanation:

Isolating the server will prevent further intrusions and protect evidence of intrusion activities left in memory and on the hard drive. Some intrusion activities left in virtual memory may be lost if the system is shut down. Duplicating the hard disk will only preserve the evidence on the hard disk, not the evidence in virtual memory, and will not prevent further unauthorized access attempts. Copying the database log file to a protected server will not provide sufficient evidence should the organization choose to pursue legal recourse.

QUESTION NO: 1406

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

A.
Setting up a backup site

B.
Maintaining redundant systems

C.
Aligning with recovery time objectives (RTOs)

D.
Data backup frequency

Answer: C
Explanation:

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

QUESTION NO: 1407

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

Answer: C
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 NO: 1408

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

A.
The independence of the investigator

B.
Timely intervention

C.
Identifying the perpetrator

D.
Chain of custody

Answer: D
Explanation:

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

QUESTION NO: 1409

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

A.
Perform a backup of the suspect media to new media.

B.
Perform a bit-by-bit image of the original media source onto new media.

C.
Make a copy of all files that are relevant to the investigation.

D.
Run an error-checking program on all logical drives to ensure that there are no disk errors.

Answer: B
Explanation:

The original hard drive or suspect media should never be used as the source for analysis. The source or original media should be physically secured and only used as the master to create a bit-by-bit image. The original should be stored using the appropriate procedures, depending on location. The image created for forensic analysis should be used. A backup does not preserve 100 percent of the data, such as erased or deleted files and data in slack space — which may be critical to the investigative process. Once data from the source are altered, they may no longer be admissible in court. Continuing the investigation, documenting the date, time and data altered, are actions that may not be admissible in legal proceedings. The organization would need to know the details of collecting and preserving forensic evidence relevant to their jurisdiction.

QUESTION NO: 1410

Which of the following recovery strategies has the GREATEST chance of failure?

A.
Hot site

B.
Redundant site

C.
Reciprocal arrangement

D.
Cold site

Answer: C
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 NO: 1411

Recovery point objectives (RPOs) can be used to determine which of the following?

A.
Maximum tolerable period of data loss

B.
Maximum tolerable downtime

C.
Baseline for operational resiliency

D.
Time to restore backups

Answer: A
Explanation:

The RPO is determined based on the acceptable data loss in the case of disruption of operations. It indicates the farthest point in time prior to the incident to which it is acceptable to recover the data. RPO effectively quantifies the permissible amount of data loss in the case of interruption. It also dictates the frequency of backups required for a given data set since the smaller the allowable gap in data, the more frequent that backups must occur.

QUESTION NO: 1412

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

A.
Preparedness tests

B.
Paper tests

C.
Full operational tests

D.
Actual service disruption

Answer: A

Explanation:

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

QUESTION NO: 1413

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

A.
Assigning responsibility for acquiring the data

B.
Locating the data and preserving the integrity of the data

C.
Creating a forensically sound image

D.
Issuing a litigation hold to all affected parties

Answer: B
Explanation:

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

QUESTION NO: 1414

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

A.
Identify a recognized forensics software tool to create the image.

B.
Establish a chain of custody log.

C.
Connect the hard drive to a write blocker.

D.
Generate a cryptographic hash of the hard drive contents.

Answer: B
Explanation:

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

QUESTION NO: 1415

Which of the following is the initial step in creating a firewall policy?

A.
A cost-benefit analysis of methods for securing the applications

B.
Identification of network applications to be externally accessed

C.
Identification of vulnerabilities associated with network applications to be externally accessed

D.
Creation of an applications traffic matrix showing protection methods

Answer: B
Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

QUESTION NO: 1416

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A.
User management coordination does not exist.

B.
Specific user accountability cannot be established.

C.

Unauthorized users may have access to originate, modify or delete data.

D.
Audit recommendations may not be implemented.

Answer: C
Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

QUESTION NO: 1417

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

Answer: B
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 NO: 1418

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

Answer: B
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 NO: 1419

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.

Answer: D

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 NO: 1420

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A.
Assimilation of the framework and intent of a written security policy by all appropriate parties

B.
Management support and approval for the implementation and maintenance of a security policy

C.
Enforcement of security rules by providing punitive actions for any violation of security rules

D.
Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

QUESTION NO: 1421

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

Answer: C

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 NO: 1422

Which of the following reduces the potential impact of social engineering attacks?

A.
Compliance with regulatory requirements

B.
Promoting ethical understanding

C.
Security awareness programs

D.
Effective performance incentives

Answer: C

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

QUESTION NO: 1423

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A.
Deleting database activity logs

B.
Implementing database optimization tools

C.
Monitoring database usage

D.
Defining backup and recovery procedures

Answer: A

Explanation:

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

QUESTION NO: 1424

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

Answer: B
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 NO: 1425

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

Answer: A
Explanation:

QUESTION NO: 1426

An information security manager that is utilizing a public cloud is performing a root cause investigation of an incident that took place in that environment. Which of the following should be the security manager's **MAIN** concern?

A.
Limited access to information

B.
Shared infrastructure with other subscribers

C.
Transaction records split into multiple cloud locations

D.
Lack of security log filtering

Answer: A
Explanation:

QUESTION NO: 1427

The **PRIMARY** objective of performing a post-incident review is to:

A.
identify the root cause.

B.
identify control improvements.

C.
re-evaluate the impact of incidents.

D.
identify vulnerabilities.

Answer: B
Explanation:

QUESTION NO: 1428

Which of the following is the **MOST** important objective of testing a security incident response plan?

A.
Confirm that systems are recovered in the proper order.

B.
Verify the response assumptions are valid.

C.
Ensure the thoroughness of the response plan.

D.
Validate the business impact analysis.

Answer: C

Explanation:

QUESTION NO: 1429

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

Answer: B

Explanation:

QUESTION NO: 1430

A risk profile support effective security decisions **PRIMARILY** because it:

A.
defines how the best mitigate future risks.

B.
identifies priorities for risk reduction.

C.
enables comparison with industry best practices.

D.
describes security threats.

Answer: B
Explanation:

QUESTION NO: 1431

The **PRIMARY** goal of a post-incident review should be to:

A.
determine why the incident occurred.

B.
determine how to improve the incident handling process.

C.
identify policy changes to prevent a recurrence.

D.
establish the cost of the incident to the business.

Answer: C
Explanation:

QUESTION NO: 1432

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

Answer: D
Explanation:

QUESTION NO: 1433

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

Answer: B
Explanation:

QUESTION NO: 1434

When establishing escalation processes for an organization’s computer security incident response team, the organization’s procedures should:

A.
provide unrestricted communication channels to executive leadership to ensure direct access.

B.
require events to be escalated whenever possible to ensure that management is kept informed.

C.
recommend the same communication path for events to ensure consistency of communication.

D.
specify step-by-step escalation paths to ensure an appropriate chain of command.

Answer: D

Explanation:

QUESTION NO: 1435

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.

Answer: A

Explanation:

QUESTION NO: 1436

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

Answer: D

Explanation:

QUESTION NO: 1437

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

Answer: A

Explanation:

QUESTION NO: 1438

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

Answer: C
Explanation:

QUESTION NO: 1439

Which of the following is the **MOST** important security consideration when developing an incident response strategy with a cloud provider?

A.
Escalation processes

B.
Security audit reports

C.
Technological capabilities

D.
Recovery time objective (RTO)

Answer: C
Explanation:

QUESTION NO: 1440

Which of the following is a **MAIN** security challenge when conducting a post-incident review related to bring your own device (BYOD) in a mature, diverse organization?

A.
Ability to obtain possession of devices

B.
Lack of mobile forensics expertise

C.
Diversity of operating systems

D.
Ability to access devices remotely

Answer: C
Explanation:

QUESTION NO: 1441

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.

Answer: B
Explanation:

QUESTION NO: 1442

The **MOST** important reason to use a centralized mechanism to identify information security incidents is to:

A.
comply with corporate policies.

B.
prevent unauthorized changes to networks.

C.
detect threats across environments.

D.
detect potential fraud.

Answer: A
Explanation:

QUESTION NO: 1443

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

Answer: D
Explanation:

QUESTION NO: 1444

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

Answer: D
Explanation:

QUESTION NO: 1445

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.

Answer: D
Explanation:

QUESTION NO: 1446

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.

Answer: A
Explanation:

QUESTION NO: 1447

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

Answer: B
Explanation:

QUESTION NO: 1448

An incident response team has determined there is a need to isolate a system that is communicating with a known malicious host on the Internet.

Which of the following stakeholders should be contacted **FIRST**?

A.
Executive management

B.
System administrator

C.
Key customers

D.
The business owner

Answer: B
Explanation:

QUESTION NO: 1449

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

Answer: B
Explanation:

QUESTION NO: 1450

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.

Answer: D
Explanation:

QUESTION NO: 1451

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.

Answer: C
Explanation:

QUESTION NO: 1452

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

Answer: A

Explanation:

QUESTION NO: 1453

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.

Answer: C

Explanation:

QUESTION NO: 1454

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

Answer: A
Explanation:

QUESTION NO: 1455

Which of the following is the **MOST** important reason to consider the role of the IT service desk when developing incident handling procedures?

A.
Service desk personnel have information on how to resolve common systems issues.

B.
The service desk provides a source for the identification of security incidents.

C.
The service desk provides information to prioritize systems recovery based on user demand.

D.
Untrained service desk personnel may be a cause of security incidents.

Answer: B
Explanation:

QUESTION NO: 1456

A user reports a stolen personal mobile device that stores sensitive corporate data. Which of the following will **BEST** minimize the risk of data exposure?

A.
Wipe the device remotely.

B.
Remove user’s access to corporate data.

C.
Prevent the user from using personal mobile devices.

D.
Report the incident to the police.

Answer: A

Explanation:

QUESTION NO: 1457

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

Answer: B

Explanation:

QUESTION NO: 1458

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

Answer: B
Explanation:

QUESTION NO: 1459

After the occurrence of a major information security incident, which of the following will **BEST** help an information security manager determine corrective actions?

A.
Calculating cost of the incident

B.
Conducting a postmortem assessment

C.
Preserving the evidence

D.
Performing am impact analysis

Answer: D
Explanation:

QUESTION NO: 1460

Which of the following metrics is **MOST** appropriate for evaluating the incident notification process?

A.
Average total cost of downtime per reported incident

B.

Average number of incidents per reporting period

C.
Elapsed time between response and resolution

D.
Elapsed time between detection, reporting and response

Answer: D
Explanation:

QUESTION NO: 1461

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.

Answer: B
Explanation:

QUESTION NO: 1462

Which of the following be **MOST** effective in reducing the financial impact following a security breach leading to data disclosure?

A.

A business continuity plan

B.
Backup and recovery strategy

C.
A data loss prevention (DLP) solution

D.
An incident response plan

Answer: D
Explanation:

QUESTION NO: 1463

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

Answer: A
Explanation:

QUESTION NO: 1464

Which of the following **BEST** facilitates the effective execution of an incident response plan?

A.
The response team is trained on the plan.

B.
The plan is based on risk assessment results.

C.
The incident response plan aligns with the IT disaster recovery plan.

D.
The plan is based on industry best practice.

Answer: B
Explanation:

QUESTION NO: 1465

An information security manager developing an incident response plan **MUST** ensure it includes:

A.
an inventory of critical data

B.
criteria for escalation

C.
critical infrastructure diagrams

D.
a business impact analysis

Answer: B
Explanation:

QUESTION NO: 1466

In a cloud technology environment, which of the following would pose the **GREATEST** challenge to the investigation of security incidents?

A.
Access to the hardware

B.

Data encryption

C.
Non-standard event logs

D.
Compressed customer data

Answer: A
Explanation:

QUESTION NO: 1467

What is the **MAIN** reason for an organization to develop an incident response plan?

A.
Trigger immediate recovery procedures.

B.
Identify training requirements for the incident response team.

C.
Prioritize treatment based on incident criticality.

D.
Provide a process for notifying stakeholders of the incident.

Answer: A
Explanation:

QUESTION NO: 1468

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

Answer: C
Explanation:

QUESTION NO: 1469

An information security manager has been asked to determine whether an information security initiative has reduced risk to an acceptable level. Which of the following activities would provide the **BEST** information for the information security manager to draw a conclusion?

A.
Initiating a cost-benefit analysis of the implemented controls

B.
Reviewing the risk register

C.
Conducting a business impact analysis (BIA)

D.
Performing a risk assessment

Answer: D
Explanation:

QUESTION NO: 1470

With limited resources in the information security department, which of the following is the **BEST** approach for managing security risk?

A.
Implement technical solutions to automate security management activities.

B.

Prioritize security activities and report to management.

C.
Hire additional information security staff.

D.
Engage a third-party company to provide security support.

Answer: B
Explanation:

QUESTION NO: 1471

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).

Answer: C
Explanation:

QUESTION NO: 1472

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

Answer: C

Explanation:

QUESTION NO: 1473

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

Answer: A

Explanation:

QUESTION NO: 1474

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

Answer: C
Explanation:

QUESTION NO: 1475

Executive leadership has decided to engage a consulting firm to develop and implement a comprehensive security framework for the organization to allow senior management to remain focused on business priorities. Which of the following poses the **GREATEST** challenge to the successful implementation of a new security governance framework?

A.
Information security management does not fully accept the responsibility for information security governance.

B.
Executive leadership views information security governance primarily as a concern of the information security management team.

C.
Information security staff has little or no experience with the practice of information security governance.

D.
Executive leadership becomes involved in decisions about information security governance.

Answer: A
Explanation:

QUESTION NO: 1476

Which of the following is the **MOST** effective way to ensure information security policies are followed?

A.
Require sign-off on acceptable use policies.

B.
Require regular security awareness training.

C.
Provide detailed security procedures.

D.
Perform a gap analysis.

Answer: C
Explanation:

QUESTION NO: 1477

Which of the following is the **MOST** effective way to address an organization's security concerns during contract negotiations with a third party?

A.
Ensure security is involved in the procurement process.

B.
Communicate security policy with the third-party vendor.

C.
Review the third-party contract with the organization's legal department.

D.
Conduct an information security audit on the third-party vendor.

Answer: A
Explanation:

QUESTION NO: 1478

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.

Answer: D
Explanation:

QUESTION NO: 1479

Organization XYZ, a lucrative, Internet-only business, recently suffered a power outage that lasted two hours. The organization's data center was unavailable in the interim. In order to mitigate risk in the **MOST** cost-efficient manner, the organization should:

A.
plan to operate at a reduced capacity from the primary place of business.

B.
create an IT hot site with immediate fail-over capability.

C.
install an uninterruptible power supply (UPS) and generator.

D.
set up a duplicate business center in a geographically separate area.

Answer: C
Explanation:

QUESTION NO: 1480

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

Answer: C
Explanation:

QUESTION NO: 1481

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

Answer: A
Explanation:

QUESTION NO: 1482

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.

Answer: A
Explanation:

QUESTION NO: 1483

Which of the following is the **BEST** reason for reevaluating an information security program?

A.
Ineffectiveness of the information security strategy execution

B.
Misalignment between information security priorities and business objectives

C.
Change in senior management

D.
Noncompliance with information security policies and procedures

Answer: B
Explanation:

QUESTION NO: 1484

For an enterprise implementing a bring your own device (BYOD) program, which of the following would provide the **BEST** security of corporate data residing on unsecured mobile devices?

A.

Acceptable use policy

B.
Device certification process

C.
Containerization solution

D.
Data loss prevention (DLP)

Answer: D
Explanation:

QUESTION NO: 1485

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.

Answer: D
Explanation:

QUESTION NO: 1486

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

Answer: A
Explanation:

QUESTION NO: 1487

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

Answer: A
Explanation:

QUESTION NO: 1488

When developing an escalation process for an incident response plan, the information security manager should **PRIMARILY** consider the:

A.
media coverage.

B.
availability of technical resources.

C.
incident response team.

D.
affected stakeholders.

Answer: C
Explanation:

QUESTION NO: 1489

Which of the following would be the **BEST** way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

A.
Perform a penetration test to demonstrate the ability to protect.

B.
Perform industry research annually and document the overall ranking of the IPS.

C.
Establish and present appropriate metrics that track performance.

D.
Provide yearly competitive pricing to illustrate the value of the IPS.

Answer: C
Explanation:

QUESTION NO: 1490

An organization utilizes a third party to classify its customers' personally identifiable information (PII). What is the **BEST** way to hold the third party accountable for data leaks?

A.
Include detailed documentation requirements within the formal statement of work.

B.
Submit a formal request for proposal (RFP) containing detailed documentation of requirements.

C.
Ensure a nondisclosure agreement is signed by both parties' senior management.

D.
Require the service provider to sign off on the organization's acceptable use policy.

Answer: A

Explanation:

QUESTION NO: 1491

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.

Answer: D

Explanation:

QUESTION NO: 1492

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

A.
Invoke the organization's incident response plan.

B.
Set up communication channels for the target audience.

C.
Determine the needs and requirements of each audience.

D.
Create a comprehensive singular communication.

Answer: C
Explanation:

QUESTION NO: 1493

When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the **MOST** valuable input?

A.
Recommendations from senior management

B.
The business continuity plan (BCP)

C.
Business impact analysis (BIA) results

D.
Vulnerability assessment results

Answer: C
Explanation:

QUESTION NO: 1494

An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:

A bad actor broke into a business-critical FTP server by brute forcing an administrative password

The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored

The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server

After three (3) hours, the bad actor deleted the FTP directory causing incoming FTP attempts by legitimate customers to fail

Which of the following poses the **GREATEST** risk to the organization related to this event?

A.
Removal of data

B.
Downtime of the service

C.
Disclosure of stolen data

D.
Potential access to the administration console

Answer: B

Explanation:

QUESTION NO: 1495

An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's **FIRST** course of action?

A.
Shut down the server in an organized manner.

B.
Validate that there has been an incident.

C.
Inform senior management of the incident.

D.
Notify the business process owner.

Answer: B
Explanation:

QUESTION NO: 1496

An information security manager has been alerted to a possible incident involving a breach at one of the organization's vendors. Which of the following should be done **FIRST**?

A.
Discontinue the relationship with the vendor.

B.
Perform incident recovery.

C.
Perform incident eradication.

D.
Engage the incident response team.

Answer: D
Explanation:

QUESTION NO: 1497

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

Answer: D

Explanation:

QUESTION NO: 1498

After a security incident has been contained, which of the following should be done **FIRST**?

A.
Conduct forensic analysis

B.
Notify local authorities

C.
Restore the affected system from backup

D.
Perform a complete wipe of the affected system

Answer: C

Explanation:

QUESTION NO: 1499

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

Answer: B

Explanation:

QUESTION NO: 1500

Which of the following would be the **MOST** effective incident response team structure for an organization with a large headquarters and worldwide branch offices?

A.
Centralized

B.
Coordinated

C.
Outsourced

D.
Decentralized

Answer: B

Explanation:

QUESTION NO: 1501

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

Answer: C

Explanation:

QUESTION NO: 1502

Which of the following should be communicated **FIRST** to senior management once an information security incident has been contained?

A.
Whether the recovery time objective was met

B.
A summary of key lessons learned from the incident

C.
The initial business impact of the incident

D.
Details on containment activities

Answer: C

Explanation:

QUESTION NO: 1503

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

Answer: B

Explanation:

QUESTION NO: 1504

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

Answer: D

Explanation:

QUESTION NO: 1505

What is the **PRIMARY** purpose of communicating business impact to an incident response team?

A.
To provide monetary values for post-incident review

B.
To provide information for communication of incidents

C.
To facilitate resource allocation for preventive measures

D.
To enable effective prioritization of incidents

Answer: D

Explanation:

QUESTION NO: 1506

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.

Answer: B

Explanation:

QUESTION NO: 1507

An organization's security was compromised by outside attackers. The organization believed that the incident was resolved. After a few days, the IT staff is still noticing unusual network traffic. Which of the following is the **BEST** course of action to address this situation?

A.
Initiate the incident response process.

B.
Identify potential incident impact.

C.
Implement additional incident response monitoring tools.

D.
Assess the level of the residual risk.

Answer: A

Explanation:

QUESTION NO: 1508

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

Answer: B

Explanation:

QUESTION NO: 1509

Which of the following would **BEST** demonstrate the maturity level of an organization's security incident response program?

A.
An increase in the number of reported incidents

B.
A decrease in the number of reported incidents

C.
A documented and live-tested incident response process

D.
Ongoing review and evaluation of the incident response team

Answer: C

Explanation:

QUESTION NO: 1510

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

Answer: D

Explanation:

QUESTION NO: 1511

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.

Answer: D

Explanation:

QUESTION NO: 1512

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.

Answer: A
Explanation:

QUESTION NO: 1513

An information security manager is preparing an incident response plan. Which of the following is the **MOST** important consideration when responding to an incident involving sensitive customer data?

A.
The assignment of a forensics team

B.
The ability to recover from the incident in a timely manner

C.
The ability to obtain incident information in a timely manner

D.
Following defined post-incident review procedures

Answer: D

Explanation:

QUESTION NO: 1514

Which of the following is the **BEST** way to prevent recurrence of a security incident?

A.
Review and update security policy on a regular basis

B.
Management support and approval of the incident response plan

C.
An appropriate investigation into the root cause with corrective measures applied

D.
An expanded and more effective monitoring and detection process for incidents

Answer: C

Explanation:

QUESTION NO: 1515

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.

Answer: C

Explanation:

QUESTION NO: 1516

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.

Answer: D

Explanation:

QUESTION NO: 1517

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

Answer: A

Explanation:

QUESTION NO: 1518

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.

Answer: B

Explanation:

QUESTION NO: 1519

An organization was forced to pay a ransom to regain access to a critical database that had been encrypted in a ransomware attack. What would have **BEST** prevented the need to make this ransom payment?

A.
Storing backups on a segregated network

B.
Training employees on ransomware

C.
Ensuring all changes are approved

D.
Verifying the firewall is configured properly

Answer: A

Explanation:

QUESTION NO: 1520

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

Answer: A

Explanation:

QUESTION NO: 1521

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.

Answer: A

Explanation:

QUESTION NO: 1522

Information classification is a fundamental step in determining:

A.
whether risk analysis objectives are met.

B.
who has ownership of information.

C.
the type of metrics that should be captured.

D.
the security strategy that should be used.

Answer: B
Explanation:

QUESTION NO: 1523

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

Answer: A

Explanation:

QUESTION NO: 1524

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

Answer: C

Explanation:

QUESTION NO: 1525

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

Answer: D

Explanation:

QUESTION NO: 1526

Which of the following is the **MOST** important component of information security governance?

A.
Approved Information security strategy

B.
Documented information security policies

C.
Comprehensive information security awareness program

D.
Appropriate information security metrics

Answer: D

Explanation:

QUESTION NO: 1527

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.

Answer: D

Explanation:

QUESTION NO: 1528

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.

Answer: D
Explanation:

QUESTION NO: 1529

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.

Answer: D

Explanation:

QUESTION NO: 1530

Which of the following is **MOST** important to the successful development of an information security strategy?

A.
A well-implemented governance framework

B.
Current state and desired objectives

C.
An implemented development life cycle process

D.
Approved policies and standards

Answer: A
Explanation:

QUESTION NO: 1531

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.

Answer: B

Explanation:

QUESTION NO: 1532

When aligning an organization's information security program with other risk and control activities, it is **MOST** important to:

A.
develop an information security governance framework.

B.
have information security management report to the chief risk officer.

C.
ensure adequate financial resources are available.

D.
integrate security within the system development life cycle.

Answer: A
Explanation:

QUESTION NO: 1533

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.

Answer: A

Explanation:

QUESTION NO: 1534

An information security manager has determined that the mean time to prioritize information security incidents has increased to an unacceptable level. Which of the following processes would **BEST** enable the information security manager to address this concern?

A.
Incident classification

B.
Vulnerability assessment

C.
Incident response

D.
Forensic analysis

Answer: A

Explanation:

QUESTION NO: 1535

Which of the following is the **PRIMARY** responsibility of the information security manager when an organization implements the use of personally-owned devices on the corporate network?

A.
Requiring remote wipe capabilities

B.
Enforcing defined policy and procedures

C.
Conducting security awareness training

D.
Encrypting the data on mobile devices

Answer: B

Explanation:

QUESTION NO: 1536

During an information security audit, it was determined that IT staff did not follow the established standard when configuring and managing IT systems. Which of the following is the **BEST** way to prevent future occurrences?

A.
Updating configuration baselines to allow exceptions

B.
Conducting periodic vulnerability scanning

C.
Providing annual information security awareness training

D.
Implementing a strict change control process

Answer: D

Explanation:

QUESTION NO: 1537

Which of the following should be the **PRIMARY** focus of a post-incident review following a successful response to a cybersecurity incident?

A.
Which control failures contributed to the incident

B.
How incident response processes were executed

C.
What attack vectors were utilized

D.
When business operations were restored

Answer: D

Explanation:

QUESTION NO: 1538

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.

Answer: C

Explanation:

QUESTION NO: 1539

Which of the following is the **MOST** important reason for performing a cost-benefit analysis when implementing a security control?

A.
To present a realistic information security budget

B.
To ensure that benefits are aligned with business strategies

C.
To ensure that the mitigation effort does not exceed the asset value

D.
To justify information security program activities

Answer: B

Explanation:

QUESTION NO: 1540

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.

Answer: B

Explanation:

QUESTION NO: 1541

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.

Answer: D

Explanation:

QUESTION NO: 1542

An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is **MOST** important to establish:

A.
automated reporting to stakeholders.

B.
a control self-assessment process.

C.
metrics for each milestone.

D.
a monitoring process for the security policy.

Answer: C

Explanation:

QUESTION NO: 1543

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.

Answer: A

Explanation:

QUESTION NO: 1544

For an organization that is experiencing outages due to malicious code, which of the following is the **BEST** index of the effectiveness of countermeasures?

A.
Number of virus infections detected

B.
Amount of infection-related downtime

C.
Average recovery time per incident

D.
Number of downtime-related help desk calls

Answer: B

Explanation:

QUESTION NO: 1545

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.

Answer: A

Explanation:

QUESTION NO: 1546

During an incident, which of the following entities would **MOST** likely be contacted directly by an organization's incident response team without management approval?

A.
Industry regulators

B.
Technology vendor

C.
Law enforcement

D.
Internal audit

Answer: D

Explanation:

QUESTION NO: 1547

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.

Answer: A

Explanation:

QUESTION NO: 1548

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.

Answer: B

Explanation:

QUESTION NO: 1549

Which of the following will provide the **MOST** guidance when deciding the level of protection for an information asset?

A.
Cost of controls

B.
Cost to replace

C.
Classification of information

D.
Impact to business function

Answer: C

Explanation:

QUESTION NO: 1550

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)

Answer: A

Explanation:

QUESTION NO: 1551

An information security manager determines the organization's critical systems may be vulnerable to a new zero-day attack. The **FIRST** course of action is to:

A.
advise management of risk and remediation cost.

B.
analyze the probability of compromise.

C.
survey peer organizations to see how they have addressed the issue.

D.
re-assess the firewall configuration.

Answer: B

Explanation:

QUESTION NO: 1552

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

Answer: C

Explanation:

QUESTION NO: 1553

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).

Answer: C

Explanation:

QUESTION NO: 1554

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

Answer: A

Explanation:

QUESTION NO: 1555

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.

Answer: B

Explanation:

QUESTION NO: 1556

Which of the following provides the **GREATEST** assurance that an organization allocates appropriate resources to respond to information security events?

A.
Threat analysis and intelligence reports

B.
Incident classification procedures

C.
Information security policies and standards

D.
An approved IT staffing plan

Answer: C
Explanation:

QUESTION NO: 1557

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.

Answer: C

Explanation:

QUESTION NO: 1558

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.

Answer: D

Explanation:

QUESTION NO: 1559

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

Answer: B

Explanation:

QUESTION NO: 1560

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the **BEST** assurance that the third party's contract programmers comply with the organization's security policies?

A.

Require annual signed agreements of adherence to security policies.

B.

Include penalties for noncompliance in the contracting agreement.

C.

Perform periodic security assessments of the contractors' activities.

D.

Conduct periodic vulnerability scans of the application.

Answer: C

Explanation:

QUESTION NO: 1561

Which of the following is a **PRIMARY** function of an incident response team?

A.

To provide a business impact assessment

B.

To provide effective incident mitigation

C.

To provide a single point of contact for critical incidents

D.

To provide a risk assessment for zero-day vulnerabilities

Answer: B

Explanation:

QUESTION NO: 1562

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

Answer: C

Explanation:

QUESTION NO: 1563

What is the **PRIMARY** purpose of an unannounced disaster recovery exercise?

A.
To evaluate how personnel react to the situation

B.
To provide metrics to senior management

C.
To estimate the recovery time objective (RTO)

D.
To assess service level agreements (SLAs)

Answer: A

Explanation:

QUESTION NO: 1564

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.

Answer: D

Explanation:

QUESTION NO: 1565

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

Answer: B

Explanation:

QUESTION NO: 1566

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.

Answer: D

Explanation:

QUESTION NO: 1567

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.

Answer: A

Explanation:

QUESTION NO: 1568

An organization has determined that one of its web servers has been compromised. Which of the following actions should be taken to preserve the evidence of the intrusion for forensic analysis and potential litigation?

A.
Reboot the server in a secure area to search for digital evidence.

B.
Unplug the server from the power.

C.
Restrict physical and logical access to the server.

D.
Run analysis tools to detect the source of the intrusion.

Answer: C
Explanation:

QUESTION NO: 1569

Which of the following is the **GREATEST** potential exposure created by outsourcing to an application service provider?

A.
Denial of service attacks

B.
Combining incompatible duties

C.
Mixing of data

D.
Lack of technical expertise

Answer: C

Explanation:

QUESTION NO: 1570

Which of the following **BEST** indicates an effective vulnerability management program?

A.
Risks are managed within acceptable limits.

B.
Threats are identified accurately.

C.
Vulnerabilities are managed proactively.

D.
Vulnerabilities are reported in a timely manner.

Answer: C

Explanation:

QUESTION NO: 1571

Which of the following would contribute **MOST** to employees' understanding of data handling responsibilities?

A.
Demonstrating support by senior management of the security program

B.
Requiring staff acknowledgement of security policies

C.
Labeling documents according to appropriate security classification

D.
Implementing a tailored security awareness training program

Answer: D

Explanation:

QUESTION NO: 1572

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

Answer: C

Explanation:

QUESTION NO: 1573

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following **MUST** be in place for this solution to be relevant to the organization?

A.
Senior management support

B.
A data classification schema

C.
An adequate data testing environment

D.
A business case

Answer: D

Explanation:

QUESTION NO: 1574

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

Answer: B
Explanation:

QUESTION NO: 1575

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

Answer: A

Explanation:

QUESTION NO: 1576

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.

Answer: C

Explanation:

QUESTION NO: 1577

An online payment provider's computer security incident response team has confirmed that a customer credit card database was breached. Which of the following is **MOST** important to include in a report to senior management?

A.
A summary of the security logs that illustrates the sequence of events

B.
An explanation of the potential business impact

C.
An analysis of similar attacks and recommended remediation

D.
A business case for implementing stronger logical access controls

Answer: B

Explanation:

QUESTION NO: 1578

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.

Answer: C

Explanation:

QUESTION NO: 1579

When a critical incident cannot be contained in a timely manner and the affected system needs to be taken offline, which of the following stakeholders **MUST** receive priority communication?

A.
System end-users

B.
System administrator

C.
Senior management

D.
Business process owner

Answer: D

Explanation:

QUESTION NO: 1580

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.

Answer: A

Explanation:

QUESTION NO: 1581

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.

Answer: D

Explanation:

QUESTION NO: 1582

Which of the following poses the **GREATEST** risk to the operational effectiveness of an incident response team?

A.
The lack of a security information and event management (SIEM) system

B.
The lack of automated communication channels

C.
The lack of delegated authority

D.
The lack of forensic investigation skills

Answer: A

Explanation:

QUESTION NO: 1583

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

Answer: A

Explanation:

QUESTION NO: 1584

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.

Answer: D
Explanation:

QUESTION NO: 1585

An organization’s ability to prevent a security incident in a Software as a Service (SaaS) cloud-computing environment is **MOST** dependent on the:

A.
ability to implement a web application firewall.

B.
ability to monitor and analyze system logs.

C.
configuration and sensitivity of an intrusion detection system (IDS).

D.
granularity with which access rights can be configured.

Answer: D

Explanation:

QUESTION NO: 1586

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

Answer: A

Explanation:

QUESTION NO: 1587

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

Answer: A

Explanation:

QUESTION NO: 1588

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.

Answer: C

Explanation:

QUESTION NO: 1589

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

Answer: A

Explanation:

QUESTION NO: 1590

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.

Answer: C

Explanation:

QUESTION NO: 1591

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.

Answer: C

Explanation: