Isaca.Premium.CISM.by.VCEplus.631q

Number: CISM VCEPlus
Passing Score: 800
Time Limit: 120 min
File Version: 4.4

Exam Code: CISM
Exam Name: Certified Information Security Manager
Certification Provider: Isaca
Corresponding Certification: CISM
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-cism/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CISM exam products and you get latest questions. We strive to deliver the best CISM exam product for top grades in your first attempt.

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

Exam A

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

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

Correct Answer: B
Section: (none)
Explanation

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 3

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance Explanation

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

QUESTION 4
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 5
Information security governance is PRIMARILY driven by:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 6
Which of the following represents the MAJOR focus of privacy regulations?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 regulator)' 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 7
Investments in information security technologies should be based on:

A. vulnerability assessments.

B. value analysis.
C. business climate.
D. audit recommendations.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 12
The MOST important component of a privacy policy is:

A. notifications.
B. warranties.
C. liabilities.
D. geographic coverage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 15
Minimum standards for securing the technical infrastructure should be defined in a security:

A. strategy.
B. guidelines.
C. model.
D. architecture.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 20
Which of the following requirements would have the lowest level of priority in information security?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 23
Which of the following is MOST likely to be discretionary?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 25
Which of the following are seldom changed in response to technological changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 32
Acceptable levels of information security risk should be determined by:

A. legal counsel.
B. security management.
C. external auditors.
D. die steering committee.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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 (ROD projections.
D. comparing spending against similar organizations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance Explanation

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

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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-bystep process of how policy and standards will be implemented.

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 70
Who in an organization has the responsibility for classifying information?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 72
Logging is an example of which type of defense against systems compromise?

A. Containment
B. Detection
C. Reaction
D. Recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
Explanation

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

QUESTION 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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 82
An outcome of effective security governance is:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 84
Who should drive the risk analysis for an organization?

A. Senior management
B. Security manager
C. Quality manager
D. Legal department

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance
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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 114
Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness.
B. It is easier to manage and control.

C. It is more responsive to business unit needs.
D. It provides a faster turnaround for security requests.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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 (TC'O)
D. Baseline comparisons

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance Explanation

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

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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 BES T approach of the information security manager?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information security governance 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 140
A risk mitigation report would include recommendations for:

A. assessment.
B. acceptance
C. evaluation.
D. quantification.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 141
A risk management program should reduce risk to:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 142
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precise.

B. security risks are subject to frequent change.
C. reviewers can optimize and reduce the cost of controls.
D. it demonstrates to senior management that the security function can add value.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 143
Which of the following BEST indicates a successful risk management practice?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 144
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 145
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 146
Which of the following will BEST protect an organization from internal security attacks?

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks

D. Employee awareness certification program

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 147
For risk management purposes, the value of an asset should be based on:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 148
In a business impact analysis, the value of an information system should be based on the overall cost:

A. of recovery.
B. to recreate.
C. if unavailable.

D. of emergency operations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 149
Acceptable risk is achieved when:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 150
The value of information assets is BEST determined by:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 151
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 152
The MOST effective way to incorporate risk management practices into existing production systems is through:

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 153
Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

A. Gap analysis
B. Risk analysis
C. Regression analysis
D. Business impact analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 154
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 155
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 156
The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

A. Mitigating controls
B. Visibility of impact
C. Likelihood of occurrence
D. Incident frequency

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Section: Information risk management 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 157
Risk acceptance is a component of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management
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 158
Risk management programs are designed to reduce risk to:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 159
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 160
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).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 161
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 162
Which of the following will BEST prevent external security attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 163
In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 164
A business impact analysis (BIA) is the BEST tool for calculating:

A. total cost of ownership.
B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 165

When residual risk is minimized:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 166
Quantitative risk analysis is MOST appropriate when assessment data:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 167
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 168
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 169
A risk analysis should:

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

D. give more weight to the likelihood vs. the size of the loss.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 170
The recovery point objective (RPO) requires which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 171
Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

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

D. Systems capacity management is not performed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 172
Which of the following BEST describes the scope of risk analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management Explanation

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

QUESTION 173
The decision as to whether a risk has been reduced to an acceptable level should be determined by:

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 174
Which of the following is the PRIMARY reason for implementing a risk management program?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 175
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Section: Information risk management 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 176
A successful risk management program should lead to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management
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 177
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 178
The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 179
Which of the following is the MOST usable deliverable of an information security risk analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 180
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 181
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 182
Which two components PRIMARILY must be assessed in an effective risk analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 183
Information security managers should use risk assessment techniques to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 184
In assessing risk, it is MOST essential to:

A. provide equal coverage for all asset types.
B. use benchmarking data from similar organizations.

C. consider both monetary value and likelihood of loss.
D. focus primarily on threats and recent business losses.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 185
When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 186
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 187
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 188
It is important to classify and determine relative sensitivity of assets to ensure that:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 189
The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 190
An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 191
When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management
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 192
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 193
The valuation of IT assets should be performed by:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management
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 194
The PRIMARY objective of a risk management program is to:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 195
After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management
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 196
When performing an information risk analysis, an information security manager should FIRST:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management Explanation

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

QUESTION 197
The PRIMARY benefit of performing an information asset classification is to:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 198
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 199
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 200
Phishing is BEST mitigated by which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 201
The security responsibility of data custodians in an organization will include:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 202
A security risk assessment exercise should be repeated at regular intervals because:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 203
Which of the following steps in conducting a risk assessment should be performed FIRST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 204
The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 205
Which of the following risks is represented in the risk appetite of an organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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 206
Which of the following would a security manager establish to determine the target for restoration of normal processing?

A. Recover)' time objective (RTO)
B. Maximum tolerable outage (MTO)
C. Recovery point objectives (RPOs)
D. Services delivery objectives (SDOs)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Section: Information risk management 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.