A. Cost reduction
B. Compliance with company policies
C. Protection of business assets
D. Increased business value

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

QUESTION 107
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
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 108
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
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 109
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
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 110
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
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 111
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
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 112
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
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 113
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
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 114
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
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 115
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
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 116
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
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 117
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
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 118
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
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 119
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
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 120
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
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 121
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