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

Correct Answer: B
Explanation:
Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

QUESTION 14
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
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 15
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
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 16
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
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 17
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
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 18
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
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 19
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
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 20
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
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 21
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
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 22
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
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 23
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
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 24
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
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 25
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
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 26
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
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 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
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 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