

Correct Answer: D

Explanation:

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

QUESTION 122

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

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 123

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

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 124

The MOST important component of a privacy policy is:

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

Correct Answer: A

Explanation:

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

geographic coverage, which are more specific.

QUESTION 125

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

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 126

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

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 127

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

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 128

Investments in information security technologies should be based on:

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

Correct Answer: B

Explanation:

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

QUESTION 129

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

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 130

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

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 131

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

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 132

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

Explanation:

The link to business objectives is the most important element 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 133

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

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 134

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

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 135

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

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 136

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

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 137

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