更に上のクオリティ
更に上のサービス!

問題集

ITEXAMPASS

https://www.itexampass.jp

１年で無料進級することに提供する

Exam : **CISM**

Title : Certified Information Security Manager

Version : DEMO

1.Which of the following should be the FIRST step in developing an information security plan?
A. Perform a technical vulnerabilities assessment
B. Analyze the current business strategy
C. Perform a business impact analysis
D. Assess the current levels of security awareness
Answer: B
Explanation:
Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

2.Senior management commitment and support for information security can BEST be obtained through presentations that:
A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best security practices.
D. tie security risks to key business objectives.
Answer: D
Explanation:
Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they are presented in terms of key business objectives.

3.The MOST appropriate role for senior management in supporting information security is the:
A. evaluation of vendors offering security products.
B. assessment of risks to the organization.
C. approval of policy statements and funding.
D. monitoring adherence to regulatory requirements.
Answer: C
Explanation:
Since the members of senior management are ultimately responsible for information security, they are the ultimate decision makers in terms of governance and direction. They are responsible for approval of major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager; in some organizations, business management is involved in these other activities, though their primary role is direction and governance.

4.Which of the following would BEST ensure the success of information security governance within an organization?
A. Steering committees approve security projects

B. Security policy training provided to all managers
C. Security training available to all employees on the intranet
D. Steering committees enforce compliance with laws and regulations
Answer: A
Explanation:
The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. Compliance with laws and regulations is part of the responsibility of the steering committee but it is not a full answer. Awareness training is important at all levels in any medium, and also an indicator of good governance.
However, it must be guided and approved as a security project by the steering committee.

5.Information security governance is PRIMARILY driven by:
A. technology constraints.
B. regulatory requirements.
C. litigation potential.
D. business strategy.
Answer: D
Explanation:
Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily in line with the business strategy.