Certified Information Security Manager

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(s): B

---

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(s): D

---

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(s): C

---

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(s): A

---

5. Information security governance is PRIMARILY driven by:

A. technology constraints.

B. regulatory requirements.

C. litigation potential.

D. business strategy.

Answer(s): D

---

6. Which of the following represents the MAJOR focus of privacy regulations?

A. Unrestricted data mining

B. Identity theft

C. Human rights protection

D. Identifiable personal data

Answer(s): D

---

7. Investments in information security technologies should be based on:

A. vulnerability assessments.

B. value analysis.

C. business climate.

D. audit recommendations.

Answer(s): B

---

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.

Answer(s): B

---

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

Answer(s): B

---

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.

Answer(s): B

---

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

Answer(s): B

---

12. The MOST important component of a privacy policy is:

A. notifications.

B. warranties.

C. liabilities.

D. geographic coverage.

Answer(s): A

---

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.

Answer(s): C

---

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.

Answer(s): C

---

15. Minimum standards for securing the technical infrastructure should be defined in a security:

A. strategy.

B. guidelines.

C. model.

D. architecture.

Answer(s): D

---

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

Answer(s): B

---

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.

Answer(s): A

---

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

Answer(s): C

---

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.

Answer(s): D

---

20. Which of the following requirements would have the lowest level of priority in information security?

A. Technical

B. Regulatory

C. Privacy

D. Business

Answer(s): A