

CISM - Certified Information Security Manager

<http://www.certleader.com/CISM-dumps.html>



1. 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

2. 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: B

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

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

Answer: A

4. 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

Answer: D

5. Security technologies should be selected PRIMARILY on the basis of their:

- A. ability to mitigate business risks
- B. evaluations in trade publications
- C. use of new and emerging technologies
- D. benefits in comparison to their costs

Answer: A

6. 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

Answer: C

7. The PRIMARY goal in developing an information security strategy is to:

- A. establish security metrics and performance monitoring.
- B. educate business process owners regarding their duties.
- C. ensure that legal and regulatory requirements are met.
- D. support the business objectives of the organization.

Answer: D

8. What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- A. Defining and ratifying the classification structure of information assets
- B. Deciding the classification levels applied to the organization's information assets
- C. Securing information assets in accordance with their classification
- D. Checking if information assets have been classified properly

Answer: A

9. An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

- A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
- B. establish baseline standards for all locations and add supplemental standards as required.
- C. bring all locations into conformity with a generally accepted set of industry best practices.
- D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Answer: B

10. 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

Answer: B

11. 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

Answer: D

12. An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

- A. Security metrics reports
- B. Risk assessment reports
- C. Business impact analysis (BIA)
- D. Return on security investment report

Answer: B

13. Which of the following is responsible for legal and regulatory liability?

- A. Chief security officer (CSO)
- B. Chief legal counsel (CLC)
- C. Board and senior management
- D. Information security steering group

Answer: C

14. Who in an organization has the responsibility for classifying information?

- A. Data custodian
- B. Database administrator
- C. Information security officer
- D. Data owner

Answer: D

15. Logging is an example of which type of defense against systems compromise?

- A. Containment
- B. Detection
- C. Reaction
- D. Recovery

Answer: B

16. Which of the following is MOST important in developing a security strategy?

- A. Creating a positive business security environment
- B. Understanding key business objectives
- C. Having a reporting line to senior management
- D. Allocating sufficient resources to information security

Answer: B

17. 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

Answer: D

18. A security manager meeting the requirements for the international flow of personal data will need to ensure:

- A. a data processing agreement.
- B. a data protection registration.

- C. the agreement of the data subjects.
- D. subject access procedures.

Answer: C

19. 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.

Answer: B

20. Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- A. it implies compliance risks.
- B. short-term impact cannot be determined.
- C. it violates industry security practices.
- D. changes in the roles matrix cannot be detected.

Answer: A

21. 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

Answer: D

22. What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

- A. Risk assessment report
- B. Technical evaluation report
- C. Business case
- D. Budgetary requirements

Answer: C

23. To achieve effective strategic alignment of security initiatives, it is important that:

- A. steering committee leadership be selected by rotation.
- B. inputs be obtained and consensus achieved between the major organizational units.
- C. the business strategy be updated periodically.
- D. procedures and standards be approved by all departmental heads.

Answer: B

24. Which of the following will BEST protect an organization from internal security attacks?

- A. Static IP addressing
- B. Internal address translation
- C. Prospective employee background checks
- D. Employee awareness certification program

Answer: C

25. Acceptable risk is achieved when:

- A. residual risk is minimized.

- B. transferred risk is minimized.
- C. control risk is minimized.
- D. inherent risk is minimized.

Answer: A

26. Which of the following results from the risk assessment process would BEST assist risk management decision making?

- A. Control risk
- B. Inherent risk
- C. Risk exposure
- D. Residual risk

Answer: D

27. Risk management programs are designed to reduce risk to:

- A. a level that is too small to be measurable.
- B. the point at which the benefit exceeds the expense.
- C. a level that the organization is willing to accept.
- D. a rate of return that equals the current cost of capital.

Answer: C

28. A risk assessment should be conducted:

- A. once a year for each business process and subprocess.
- B. every three-to-six months for critical business processes.
- C. by external parties to maintain objectivity.
- D. annually or whenever there is a significant change.

Answer: D

29. Identification and prioritization of business risk enables project managers to:

- A. establish implementation milestones.
- B. reduce the overall amount of slack time.
- C. address areas with most significance.
- D. accelerate completion of critical paths.

Answer: C

30. Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

- A. Systems operation procedures are not enforced
- B. Change management procedures are poor
- C. Systems development is outsourced
- D. Systems capacity management is not performed

Answer: B

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISM Exam with Our Prep Materials Via below:

<http://www.certleader.com/CISM-dumps.html>