

Part 1: MCQ and True-False questions

1. **True** or False: Data integrity can be affected by virus infections and data communications errors.
2. What is the name of the process that is used to establish whether or not a user's identity is legitimate?
 - A. Availability
 - B. Accountability
 - C. Authorization
 - D. **Authentication**
3. Which of the following terms can be used to describe trade secrets, copyrights, trademarks, and patents?
 - A. Quality of service
 - B. Availability
 - C. **Intellectual property**
 - D. Competitive intelligence
4. A person who has authorization from an organization to test its information systems and network defence is known as which of the following?
 - A. script kiddie
 - B. **penetration tester**
 - C. professional hacker
 - D. packet monkey
5. What type of malware actually evolves, changing its size and other external file characteristics to elude detection by antivirus programs?
 - A. Trojan horse
 - B. trap door
 - C. **polymorphic threat**
 - D. macro virus

6. Which is NOT one of the core principles in traditional management theory?

A. Staffing

B. Leading

C. Directing

D. Controlling

7. What is the name for an intermediate point in a planning process, at which progress towards a goal can be measured?

A. Break point

B. Stop point

C. Objective

D. Directive

8. Which management function is dedicated to the structuring of resources to support the

accomplishment of objectives?

A. Organizing

B. Controlling

C. Planning

D. Leading

9. In which of the following policies would you find sets of rules that define acceptable behaviour within a specific organizational resource, such as Internet usage?

A. System-Specific Policies

B. Issue-Specific Security Policies

C. Enterprise Information Security Policy

D. Security Awareness Policy

10. The study of choices that have been made by individuals in the past is known as which of the following?

A. Normative Ethics

B. Applied Ethics

C. Meta-Ethics

D. Descriptive Ethics

11. Which of the following is a collection of statutes that regulates the interception of wire, electronic, and oral communications?

A. Federal Privacy Act

B. Copyright Act

C. Security and Freedom Through Encryption Act

D. Electronic Communications Privacy Act (ECPA)

12. All but which of the following is one of the five fundamental privacy principles of HIPAA?

A. Public control of medical information

B. Boundaries on the use of medical information

C. Balance of public responsibility for the use of medical information

D. Security of health information

13. Which of the six PCI DSS standard areas includes the requirement of using maintained and updated malware and anti-virus protection?

A. Cardholder Data Protection

B. Vulnerability Management Program Maintenance

C. Strong Access Control Measure Implementation

D. Network Monitoring and Testing

14. **True** or False: Liability can be applied to conduct even when no law or contract has been breached.

15. A court's right to hear a case if an act was committed in its territory or involving its citizenry is known as which of the following?

A. restitution

B. jurisdiction

C. diligence

D. due care

16. What act increased the Secret Service's role in investigating fraud and related activity

in connection with computers?

- A. PATRIOT Act
- B. Digital Millennium Copyright Act
- C. Computer Fraud and Abuse Act
- D. Sarbanes-Oxley Act

17. Which of the following is the most complex part of the digital forensics investigation process?

- A. Identify relevant items
- B. Acquire the evidence
- C. Authenticate the recovered evidence
- D. Analyze the data

18. Which of the following is used to declare the intended areas of operation for a business?

- A. Values statement
- B. Vision statement
- C. Objectives statement
- D. Mission Statement

19. True or False: Organizational planning should make use of a bottom-up process in which the employees choose the initiatives the organization should pursue.

20. A multi-layered approach to strategic planning encompasses two key objectives: general strategy and which of the following?

- A. overall strategic planning
- B. Archived profiling
- C. Organizational profiling
- D. InfoSec planning

21. Which of the following best describes a stakeholder?

- A. An individual or group that owns financial stock in an organization
- B. A competing organization
- C. An individual who buys an organization's products
- D. An individual or group who has a vested interest

22. Which of the following is used to establish a formal set of organizational principles and qualities for an organization?

- A. Values statement
- B. Vision statement
- C. Mission statement
- D. Morals statement

23. True or False: InfoSec objectives must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach.

24. According to the IDEAL framework, which functional role should be responsible for communicating policies to employees and coordinate training?

- A. Chief Executive Officer
- B. Chief Risk Officer
- C. Mid-Level Manager
- D. Enterprise Staff

25. Which of the following governance processes, as outlined in ISO 27014:2013, involves the review and assessment of organizational information security performance toward goals and objectives by the governing body?

- A. Monitor
- B. Direct
- C. Communicate
- D. Assure

26. Why is the bottom-up approach less effective than the top-down approach?

- A. Lack of technical support

B. Lack of management support

C. Lack of stakeholder support

D. Lack of stockholder support

27. Which type of security policy sets the strategic direction, scope, and tone for an organization's security efforts?

A. System-specific security policy

B. Issue-specific security policy

C. Enterprise information security policy

D. Strategic planning security policy

28. True or False: Most modern server operating systems translate ACLs into configuration sets that administrators can use to control access to their systems.

29. Which of the following is NOT a typical permission available for use in ACLs?

A. Read

B. Write

C. Delete

D. Expunge

30. Which of the following is NOT a specific characteristic of ISSP?

A. It addresses specific technology-based resources

B. It requires frequent updates

C. It addresses hardware implementation issues

D. It contains an issue statement

Part 2: Scenario-based question

Evaluate the effectiveness of the following components in building a robust information security solution. In your answer, consider their purpose, implementation challenges, benefits, limitations, and impact on organisational resilience. Provide examples where relevant to support your evaluation:

- i. Training and Awareness Programs – Discuss how employees’ education, specific training, and ongoing awareness initiatives contribute to preventing cyberattacks, incidents, improving response times, and fostering a security-conscious culture. Evaluate their effectiveness in ensuring that employees understand their responsibilities during a contingency.
- ii. Simulation, Testing and Policies – Analyse the role of exercises such as tabletop simulations, penetration testing, and disaster recovery drills in validating the contingency plan. Evaluate how policies strengthen response information security solutions and frameworks.
- iii. Post-Incident Review and Lessons Learned – Examine how systematic post-incident reviews, root cause analysis, and incorporation of lessons learned improve future information security solutions. Evaluate the effectiveness of feedback loops in updating policies, procedures, and training based on lessons learned from real-world incidents and attacks.