COLLEGE OF ENGINEERING AND APPLIED SCIENCES (CEAS)

NCIS 207 FUNDAMENTALS OF INFORMATION SECURITY

END OF SECOND SEMESTER EXAMINATION

APRIL 2025

LECTURER: MRS L. FUNDISI

DURATION: 3HRS

INSTRUCTIONS

Answer**:** **All** questions from **Section A (compulsory) [25 marks**]

: **All** questions from **Section B (compulsory) [25 marks]**

:**ANY 2 (two)** questions from **Section C** [**50 marks**]

Begin your answer to each question on a fresh page.

Section A Compulsory

Answer All QUESTIONS

1. The ultimate purpose of IT governance is to:

A. encourage optimal use of IT.
B. reduce IT costs.
C. decentralize IT resources across the organization
D. centralize control of IT

2. An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirements.
B. whether proposed system functionality is adequate.
C. the stability of existing software.
D. the complexity of installed technology.

3. **Which of the following is an example of a Confidentiality control?**

A. Firewall
B. Data encryption
C. Intrusion Detection System (IDS)
D. Redundant servers

4. What is the purpose of hashing in the context of the CIA Triad?

A. To ensure data availability
B. To verify data integrity
C. To protect data confidentiality
D. To prevent unauthorized access

5. A ransomware attack primarily impacts which component of the CIA Triad?

A. Confidentiality
B. Integrity
C. Availability
D. All of the above

6. Value delivery from IT to the business is MOST effectively achieved by:

A. Aligning the IT strategy with the enterprise strategy
B. Embedding accountability in the enterprise.
C. Providing a positive return on investment.

D. Establishing an enterprise wide risk management process.

7. The MOST likely effect of the lack of senior, management commitment to IT strategic planning is:

A. Lack of investment in technology
B. Lack of a methodology for systems development
C. Technology not aligning with organization objectives
D. Absence of control over technology contracts

8. Involvement of senior management is MOST important in the development of:

A. Strategic plans.
B. IT policies.
C. IT procedures.
D. Standards and guidelines.

9. Which of the following would you consider as an auditor to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.
B. does not vary from the IS department's preliminary budget.
C. complies with procurement procedures.
D. supports the business objectives of the organization.

10. When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objectives.
B. actions to reduce hardware procurement cost.
C. a listing of approved suppliers of IT contract resources.
D. a description of the technical architecture for the organization's network perimeter security.

11. Effective IT governance requires organizational structures and processes to ensure that:

A. the organization's strategies and objectives extend the IT strategy.
B. the business strategy is derived from an IT strategy.
C. IT governance is separate and distinct from the overall governance.
D. the IT strategy extends the organization's strategies and objectives.

12. As an IS auditor performing a review of an organization's governance model. Which of the following should be of MOST concern?

A. The organization's information security policy is not periodically reviewed by senior management.

B. A policy to ensure that systems are patched in a timely manner does not exist.
C. The audit committee did not review the global mission statement.
D. An organizational policy related to malware protection does not exist.

13. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.
B. a lack of a methodology for systems development.
C. technology not aligning with the organization's objectives.
D. an absence of control over technology contracts.

14. What is residual risk?

A. The risk that remains after implementing controls
B. The risk that is transferred to a third party
C. The risk that is ignored by the organization
D. The risk that is eliminated completely

15. Why is security awareness important for employees?

A. To eliminate all security risks
B. To ensure compliance with regulations
C. To reduce the likelihood of human error leading to security incidents
D. To transfer security responsibilities to a third party

16. As you are evaluating the IT governance framework of an organization. Which of the following would be the GREATEST concern?

A. Senior management has limited involvement.
B. Return on investment (ROI) is not measured.
C. Chargeback of IT cost is not consistent.
D. Risk appetite is not quantified.

17. IT governance is PRIMARILY the responsibility of the:

A. chief executive officer (CEO).
B. board of directors.
C. IT steering committee.
D. audit committee.

18. What is the formula for calculating risk?

A. Risk = Likelihood × Impact
B. Risk = Vulnerability × Threat
C. Risk = Asset Value × Threat
D. Risk = Probability × Severity

19. Which of the following is a key component of a security awareness program?

A. Installing firewalls
B. Conducting regular phishing simulations
C. Encrypting sensitive data
D. Performing penetration testing

20. Which of the following is a threat to Availability?

A. Data encryption
B. Denial of Service (DoS) attack
C. Unauthorized data modification
D. Phishing attack

21. Which of the following is NOT a component of the CIA Triad?

A. Confidentiality
B. Integrity
C. Availability
D. Accountability

22. What is the primary goal of risk management in information security?

A. To eliminate all risks
B. To identify, assess, and mitigate risks to an acceptable level
C. To transfer all risks to a third party
D. To ignore risks and focus on system performance

23. Which of the following is the first step in the risk management process?

A. Risk mitigation
B. Risk assessment
C. Risk identification
D. Risk monitoring

24. Which of the following is an example of a risk mitigation strategy?

A. Accepting the risk
B. Ignoring the risk
C. Implementing firewalls to reduce vulnerabilities
D. Transferring the risk to an insurance company

25. Which of the following is an example of a risk transfer strategy?

A. Implementing encryption
B. Purchasing cybersecurity insurance
C. Installing antivirus software
D. Conducting employee training

SECTION B COMPULSORY, *ANSWER ALL QUESTIONS* **[25marks]**

Case Study: IT Governance at XYZ Bank

Background

ABC Ltd Bank is a mid-sized financial institution that has recently expanded its digital banking services. The bank has invested heavily in IT infrastructure, mobile banking applications, and cloud computing to enhance customer experience and operational efficiency. However, ABC Ltd Bank has encountered several challenges, including:

1. Data Security Concerns – A recent audit revealed weak access controls, increasing the risk of unauthorized access to customer data.
2. Regulatory Compliance Issues – The bank failed to comply with certain data protection regulations, resulting in penalties.
3. IT Project Failures – Several IT initiatives exceeded budget and schedule, leading to financial losses.
4. Lack of IT Risk Management – The absence of a structured IT governance framework has led to inconsistent risk management practices.

Senior executives recognize the need to improve IT governance to align technology with business objectives, enhance compliance, and manage risks effectively.

Questions:

1) What is IT governance, and why is it important for ABC Ltd Bank? [5marks]
2) What *IT governance frameworks* and *standard* could the bank adopt, and how would they be beneficial? [10marks]
3) What are the key challenges ABC Ltd Bank may face in implementing IT governance, and how can they be addressed? [10marks]

Section C:
Answer any 2 (two) questions

Question 1

a. Explain in detail the steps taken to implement a security program for any organization of your choice (be industry specific). (25marks)

Question 2

a. Explain what Security Education, Training, and Awareness (SETA) is and its significance in ensuring organizational security. ? (10 marks)
b. Briefly explain challenges associated with the bottom -down approach in implementing Information Security? (15marks)

Question 3

What are the key steps involved in developing a Disaster Recovery Plan? Describe each step in detail and explain why it is essential for an effective DRP. (25 marks)

Question 4

Use examples to discuss the IAAA model and explain how its relationship with the CIA triad (25marks)

END OF EXAMINATION