AFRICA UNIVERSITY
A United Methodist-Related Institution

COLLEGE OF ENGINEERING AND APPLIED SCIENCES

NCIS207- FUNDAMENTALS OF INFORMATION SECURITY

END OF SECOND SEMESTER EXAMINATION

APRIL /MAY 2024

LECTURER: MRS L. TEMBANI-FUNDISI

DURATION: 3 HOURS

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. Information security governance is PRIMARILY driven by
   A. Technology constraints
   B. Regulatory requirements
   C. Litigation potentials
   D. Business strategy
2. Determining which element of the Confidentiality, integrity and availability (CIA) triad is MOST important necessary task when
   A. Assessing overall system risk
   B. Developing a controls policy
   C. Determining treatment options
   D. Developing a classification scheme
3. Which of the following is a characteristic of centralized information security management?
   A. More expensive to administer
   B. Better adherence to policies
   C. More responsive to business unit needs
   D. Faster turnaround of requests
4. 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
5. 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
   C. Internal auditor
   D. Legal counsel
6. Which of the following are seldom changed in response to technological changes?
   A. Standards
   B. Policies
   C. Procedures
   D. Guidelines
7. Which of the following is the MOST appropriate position to sponsor the design and implantation of a new security infrastructure in a large global enterprise?
   A. Chief security officer
   B. Chief operating officer
   C. Chief privacy officer
   D. Chief legal counsel
8. The PRIMARY goal of developing an information security strategy is to:
   A. Establish security metrics and performance monitoring
   B. Support the business objectives of the organization

C. Educate business process owners regarding their duties
D. Ensure that legal and regulatory requirements are met

9. Senior management commitment and support for information security can BEST be enhanced through:
   A. A formal security policy sponsored by the chief executive officer
   B. Periodic review of alignment with business management goals
   C. Senior management sign-off on the information security strategy
   D. A regular security awareness training for employees
10. When an information security manager is developing a strategic plan for information security, the time line for the plan should be:
   A. Aligned with the IT strategic plan
   B. Aligned with the business strategy
   C. Three to five years both hardware and software
   D. Based on the current rate of technological change
11. From an information security manager perspective, what is an immediate benefit of clearly defined roles and responsibities
   A. Enhanced policy compliance
   B. Improved procedure flows
   C. Segregation of duties
   D. Better accountability
12. Information security policy enforcement is the responsibility of the:
   A. Security steering committee
   B. Chief information security officer
   C. Chief information officer
   D. Chief compliance officer
13. Information security frameworks can be MOST useful for the information security manager because they:
   A. Provide a detailed processed and methods
   B. Provide structure and guidance
   C. Are designed to achieve specific outcomes
   D. Provide policy and procedures
14. Business goals define the strategic direction of the organization. Functional goals define the tactical direction of a business function. Security goals define the security direction of the organization. What is the MOST important relationship between these concepts?
   A. Functional goals should be derived from the security goals
   B. Security goals should be derived from the business goals
   C. Business goals should be derived from security goals
   D. Security and business goals should be defined independently from each other
15. Which of the following choices is a necessary attribute of an effective information security governance framework?
   A. Organizational policies and guidelines in line with predefined procedures
   B. An organizational structure with minimal conflicts of interest, with sufficient resources and defined responsibilities

C. Business objectives aligned with a predefined security strategy
D. Security guidelines that address multiple facets of security such as strategy, regulatory compliance and controls

16. The enactment of policies and procedures for preventing hacker intrusions is an example of an activity that belongs to:
    A. Risk management
    B. Governance
    C. It management
    D. Compliance
17. An IS manager had decided to implement a security system to monitor access to the internet and prevent access to numerous sites. Immediately upon installation employees flood the IT help desk with complaints of being unable to perform business functions on Internet sites. This is an example of:
    A. Strong protection of information resources
    B. Conflicting security controls with organizational needs
    C. Implementing appropriate controls to reduce risk
    D. Proving information security's protective abilities
18. The data access requirements for an application should be determined by the:
    A. Legal department
    B. Business owner
    C. Information security manager
    D. Compliance officer
19. Effective governance of enterprise security is BEST ensured by:
    A. Referring the matter to the organization's legal department
    B. Using a top-down approach
    C. Management by the IT department
    D. Using bottom-up approach
20. The first step in developing a risk management program is to establish what?
    A. Management support
    B. The context and purpose of the program
    C. A security policy and procedure
    D. An oversight committee
21. What is the main objective of risk evaluation?
    A. It ensures that risks are categorized appropriately.
    B. It ensures that all the controls are effective.
    C. It provides an assessment of the risk management program.
    D. It provides a basis for selecting risk response.
22. What is the most effective strategy for risk management?
    A. To achieve a balance between risk and business goals
    B. To reduce the risk to an acceptable level
    C. To develop policy statements
    D. To document all unmitigated risks

23. What is the SDLC phase in which risk assessment should first be conducted?
    A. Implementation
    B. Feasibility
    C. Testing
    D. Programming
24. The security manager received a request to approve an exception to security standards for a proposed system change. What should be the best course of action for the security manager?

    A To reject the approval and insist on compliance with security policy
    B. To understand the risk due to non-compliance and recommend alternative controls
    C. To update the security policy and allow for the exception
    D. To provide training to the business manager on the importance of security compliance
25. How should legal and regulatory requirements be considered?

    A. As per the security policy
    B. As per business decisions
    C. As per budget availability
    D. As mandatory compliance

Section B Compulsory

Answer all questions

Case Study: Business Continuity Planning in Information Security
Company X is a global financial services organization that handles sensitive customer data and conducts transactions through its online platform. The company recognizes the importance of business continuity planning in ensuring the availability, confidentiality, and integrity of its information assets.
Scenario:
Company X recently experienced a cyberattack that resulted in a temporary disruption of its online platform. While the incident was quickly contained, it highlighted the need for a robust business continuity plan to mitigate such risks and ensure the organization can continue its operations smoothly.

Questions:

1) Why is business continuity planning essential for information security in Company X's context? [10]
2) What are the key components of a business continuity plan specific to information security? [5]
3) How can Company X identify and assess potential risks to information security? [5]
4) What measures can Company X take to mitigate and prevent information security incidents? [5]

Section C:
Answer any 2 (two) questions

Question 1

a. Explain in detail the Enterprise Information Security Policy and indicate its major components [25]

Question 2

a. Performance measure is one of the goals of Information Security Governance, describe the other 4 in detail [12]
b. What are advantages and advantages of outsourcing information systems assets [13]

Question 3

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

Question 4

What are the key steps involved in developing a DRP? Describe each step in detail and explain why it is essential for an effective DRP [25]

END OF EXAMINATION