EXAMINATION

DATE:28th May 2024 Time: 17:00-19:30 Hours

A. This examination consists of questions on material taught through the lecture sessions and associated references.
   - **Part A** (30%) is composed of 15 multiple-choice questions;
   - **Part B** (70%) with 9 questions requires detailed, complete and correct answers. Be concise with your answers by using the fewest words possible to provide detailed, complete and correct answers.
   - This examination booklet has 6 (six) pages.

B. You are required to answer all questions.

C. You must work as an individual. The order of questions neither corresponds with the order of the course material nor the associated difficulty.

D. This is a closed-book examination and no reference material is allowed in the examination room; no books, no course notes or printouts of any kind. No calculators, no cellphones/smartphones, computers, or electronic devices of any kind. You must turn off any electronic devices and store them under your desk simply having any device (even if turned off) with you during the exam constitutes a violation and will be reported. If you need to borrow a pencil, sharpener, eraser, etc., you must ask a proctor. You are not allowed to directly talk to any of your neighbours in the examination room.

E. During the examination:
   - You are not allowed to leave the examination, except for visits to the washrooms and with the permission of the proctor.
   - Do not stand up or talk until all examination scripts are picked up; should you complete the examination earlier than the allotted time, raise your hand to draw the proctor's attention to collect your examination script.
   - Ask the proctor questions that are meaningful in the context of the examination. Ensure that your questions are not probing for answers to the questions.
   - If you are found cheating, involved in discussions, talking to other students or causing any kind of disturbance during the examination, then you will be reported to appropriate university officials for violation of examination policy; you will face appropriate sanctions according to the university examination policy.
   - Answers must be properly marked in the answer book with the corresponding question number. Only answers in the answer book will be marked and graded.
   - Return both the answer/question books to the proctor before leaving the examination hall.
   - You must stop writing when the proctor announces that the allotted examination duration has expired.

Part A – Multiple Choice Questions (30 Marks)

A. Which of the following is **not true** regarding an organization's information security policy? It
   A. Establishes responsibility for all parties concerning assuring a secure environment.
   B. It delineates the role of information security in the organization.
   C. Is conceived, designed, mandated and enforced by the information security staff.
   D. It is broad and aligns with the organization's corporate and risk management objectives.

2. In managing the information security of an organization, an information security risk assessment is essential to realize the following:
   A. Determine the information security manager's view and preferences.
   B. Identify information assets and determine the value of those assets.
   C. Find asset vulnerabilities, the threats that could exploit the vulnerabilities and the potential consequences.
   D. Rank identified risks, prioritize them and the needed extra control measures.

3. What is the Annual Loss Expectancy (ALE) relating to an asset whose value (AV) is KES100,000? From past data, records of incidents that cause losses happen every two years with an exposure factor of 20%.
   A. KES100,000
   B. KES50,000
   C. KES20,000
   D. KES10,000

4. Which one of the following is NOT a meaningful risk control strategy selection?
   A. When the potential loss is significant: use design principles, architectural designs, and technical and non-technical controls to limit the degree of the attack, hence reducing the potential for loss.
   B. When the attacker's potential gain is less than the costs of attack: use protections to decrease the attacker's cost or reduce the attacker's gain, by using technical or operational controls.
   C. When there is a vulnerability: implement controls to reduce the likelihood of exploiting the vulnerability.
   D. When a vulnerability can be exploited: implement layered defenses, architectural designs, and administrative controls to reduce the risk or avert the occurrence of an attack.

5. The key outcomes of Information Security Governance include all but which one of the following?
   A. Value delivery by optimizing information security investments in support of organizational objectives

B. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.
C. Time management by aligning resources with personnel schedules and organizational objectives.
D. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved.

6. Which of the following is NOT true about planning?
   A. Operational plans and objectives are the essential input for strategic planning.
   B. Organizational mission, vision and objectives are used to create strategic plans.
   C. Tactical plans are used to create operational plans.
   D. Strategic plans are used to create tactical plans.

7. What is the best description of a stream cipher?
   A. The sender must encrypt the message with his/her private key so the receiver can decrypt it with her/his public key.
   B. The message is divided into blocks and mathematical functions are performed on each block.
   C. The cipher executes 16 rounds of computation on each bit.
   D. The cipher uses a key to create a keystream and XORs the result with the message.

8. Intrusion Detection/Prevention Systems (IDPs) perform the following well, except
   A. Recognizing activity patterns that vary from normal activity.
   B. Monitoring and analyzing system events and user behaviour.
   C. Effectively responding to attacks by sophisticated attackers.
   D. Recognizing system event patterns matching known attacks.

9. Which of the following statements is true concerning firewalls and their capability to adapt to a network environment?
   A. Given that firewalls are not programmed like a computer system, they are less error-prone.
   B. Firewalls can understand activities in the network environment and make decisions based on inferences outside their design.
   C. Firewall activity is restricted to defined patterns of measured observation
   D. Firewalls are flexible and can adapt to new threats.

10. Trusted recovery may be defined as:
    A. Securely restoring a system after a hard drive failure.
    B. Procedures that restore a system and its data in a trusted manner after the system is disrupted or a system failure occurs.
    C. An operating system regains a secure state after a brief lapse into an insecure state.

D. Finding missing equipment and verifying that security policies were not violated

11. Concerning the Information Security Management System (ISMS), which of the following controls are essential to address services provided by third parties?
    A. The third-party has to ensure that it protects the information belonging to the client organization.
    B. The organization must monitor and review the services provided by the third party to ensure the security of its information.
    C. Changes to information security agreements would be excluded from future contracts.
    D. The organization's information security guidelines must be tailored to the third party's guidelines.

12. For an Information Security Management System (ISMS), which one of the following is essential for determining the ISMS scope?
    E. The organization's legal status and location of its business.
    F. The organization's budget for information security.
    G. The organization's information assets.
    H. The technologies used in the organization.

13. Planned regular testing of an organization's disaster and recovery plan (DRP) and business continuity plan (BCP) is essential for the following reasons, except:
    A. Following a merger or acquisition.
    B. Change of laws and regulations.
    C. There is an extra money allocated for the related budget.
    D. The system and environment change.

14. An information security audit will help to:
    A. Create awareness of an organization's security policy.
    B. Identify gaps in the information security policy.
    C. Make users adhere to an organization's security policy.
    D. Prevent unauthorized users from exploiting organization resources.

15. Your organization's management team has asked for a demonstration of how well security policies, guidelines and procedures are implemented. Which of the following would be the optimal approach?
    A. Conduct an independent evaluation of the policies, guidelines and procedures.
    B. Examine test results from a range of security tests.
    C. Examine test results from the perspective of new and emerging threats.
    D. Assess test results based on the current threat landscape.

PART II – Short Answer Questions (70 Marks)

1. In security design, it is essential to balance between the security provided by a system and its ease of use. In this context, therefore: (10Marks)
   A. Explain what you understand by information security.
   B. Explain what you understand by the term usability as it applies to information systems.
   C. Why is there concern and need to balance the two?
   D. Give 2 practical examples where there is a need to balance security and usability.
2. Security planning is essential for effective information security management. Answer the following questions. (10 Marks)
   A. What do you understand by the term 'information security strategy'?
   B. Distinguish between top-down versus Bottom-Up Planning.
   C. Explain the pros and cons of Top-Down and Bottom-Up Planning.
   D. Which one (Top-Down Planning or Bottom Up Planning) is superior to the other? Explain your answer using a practical example.
3. Security Risk Management: In assessing the risks presented by vulnerabilities, vulnerability management adopts a systematic approach. Once a vulnerability has been evaluated and ranked for severity, a decision on how to deal with the vulnerability will be based on one of four strategies to manage the associated risk. (10 Marks)
   A. Explain why information security management is considered a risk management function.
   B. Name each of the four strategies.
   C. Explain each of the four strategies.
   D. Which of the four strategies is superior to all others?
4. Enterprise Architecture vs Security Architecture (10 Marks)
   A. Explain what you understand by the term Enterprise Architecture.
   B. Explain what you understand by the term Security Architecture.
   C. Describe the difference between the two.
   D. Identify the key security architecture components of an organization's security architecture.
5. Typical cryptosystems are hybrid, i.e. they employ both asymmetric and symmetric cryptosystems where the former is used for key distribution while the latter is used for sessions. Answer the following: (20 Marks)
   A. Differentiate between asymmetric and symmetric cryptosystems.

B. What are the pros and cons of each of these systems?
C. Key management is a major concern in cryptosystems. (a) define the term 'key management' and (b) discuss typical key management challenges encountered in cryptosystems.
D. What properties of an asymmetric cryptosystem make it suitable for key distribution?
E. What makes a symmetric system suitable for sessions?
F. Describe how cryptography implements digital signatures.
G. Diagrammatically illustrate a digital signature system

6. To protect information assets, organizations implement Information System Management Systems (ISMSs). (10 Marks)
   A. Explain what you understand by the term Information System Management System (ISMS).
   B. Describe the key (naming at least three) benefits of implementing an ISMS.
   C. The scope of an ISM is a major consideration of ISMS implementation.
      - Explain what you understand by the term scope.
      - Describe the guiding principles that would enable you to determine the scope of ISMS implementation in your organization.
7. Information Security Metrics: (12 Marks)
   A. Explain what you understand by the term 'security metrics'.
   B. What role do security metrics play in the management of information security?
   C. Give at least 2 examples of information security metrics.
8. Artificial Intelligence (AI) is seen to complement cyber security in the future. (12 marks)
   A. Define the term 'Artificial Intelligence'
   B. Describe (at least three) ways regarding how AI can aid security operations. Pick one of the technologies – malware detection, Intrusion Detection & Prevention System (IDPS), firewalls or Security Information Event Management System (SIEMS) – to illustrate your response.
   C. Discuss (at least two) limitations of over-reliance on AI for such functions.
9. Information Security Audit (12 Marks)
   A. What do you understand by the term information security audit?
   B. What is the role of standards in such an audit?
   C. Explain how you would proceed to conduct an information security audit.
   D. What are the limitations of such an information security audit?