Strathmore UNIVERSITY

SCHOOL OF CUMPUTING AND ENGINEERING SCIENCES
MASTER OF SCIENCE IN INFORMATION SYSTEMS SECURITY
MST 8601 INFORMATION SECURITY MANAGEMENT
END OF SEMESTER EXAMINATION

DATE: 03rd October 2022 Time: 2 Hours: 30 Minutes

A. This examination consists of questions on material taught through the lecture sessions and associated references.
   - **Part A** (30 Marks) is composed of 15 multiple choice questions;
   - **Part B** (70 Marks) with 11 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 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 room, 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 examination questions.
   - If you are found cheating, talking to other students, involved in distractions 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 back 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)

1. Which of the following is **not true** of an organization's information security policy? It:
   A. Is broad and aligns with the organization's corporate objectives.
   B. Is mandated, designed and enforced by the information security staff.
   C. Identifies and makes clear information security goals and objectives in the organization.
   D. Assigns accountability for all parties with respect to assuring a secure environment.

2. Information security planning is an essential component of information security management. Which of the follow is true about planning?
   A. Tactical plans are used to create strategic plans.
   B. Operational plans are used to create strategic plans.
   C. Strategic plans are used to create tactical plans.
   D. Operational plans are used to create tactical plans.

3. Some of the key outcomes of Information Security Governance include all of the following, except:
   A. Performance measurement by assessing, monitoring, and reporting information security governance metrics to ensure that an organization's objectives are achieved.
   B. Time management by aligning resources with personnel schedules and the organization's objectives.
   C. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.
   D. Value delivery through optimization of information security investments in support of an organization's objectives.

4. Information Security Governance is concerned with the following, except:
   A. The reported incidents and the solutions thereof.
   B. The information that needs protection and why.
   C. The strategic policies that should be created and who should carry out these policies.
   D. The risks to the information and the severity of these risks.

5. Business impact Analysis (BIA) is an essential component of contingency planning. The target audience for results of the BIA is:
   A. The contingency management team.
   B. Auditors.
   C. Everyone responsible for continuity of critical business processes.
   D. IT management team.

6. What is the best description of a stream cipher?
    A. The message is divided into blocks and mathematical functions are performed on each block.
    B. The sender must encrypt the message with his/her private key so the receiver can decrypt it with her/his public key.
    C. A cryptographic key and a specified algorithm are applied to each binary digit, one byte at a time.
    D. The cipher executes 16 rounds of computation on each bit?

7. Cryptosystems can be used to implement non-repudiation using one of the following:
    A. Public Key Infrastructure (PKI)
    B. Digital signatures
    C. Secret key
    D. Block chaining cipher

8. Which of the following best defines the term 'trusted recovery':
    A. Procedures that restore a system and its data in a trusted manner after the system was disrupted or a system failure occurred.
    B. Finding missing equipment and verifying that security policies were not violated.
    C. An operating system regaining a secure state after a brief lapse into an insecure state.
    D. Securely restoring a system after a hard drive failure.

9. 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. There is extra budget.
    B. Following a divesture of a business unit.
    C. Enactment of new laws and regulations.
    D. Acquisition new technology.

10. With respect to Information Security Management System (ISMS), what is the relationship between threats and vulnerabilities as they relate to risk?
    A. Each threat represents a vulnerability of an ISMS .
    B. Threats are associated with assets but vulnerabilities pertain to information and/or applications
    C. Threats are always external while vulnerabilities occur inside an organization.
    D. Threats exploit vulnerabilities; coupled with the chance of this occurring leads to risk

11. One of the following statements is true concerning Intrusion Detection & Intrusion Prevention Systems (IDPS) and their capability to adapt to a network environment?
    A. IDPS are flexible and can adapt to new threats.
    B. IDPS activity is restricted to defined patterns of measured observation.
    C. Given that IDPS are not programmed like a computer system, they are less error prone.
    D. IDPS can understand activities in the network environment and make decisions based on inferences outside their design.

12. Security operations include the following controls and/or processes:
    A. Incident preparedness and response.
    B. Backup of information, system images and software applications.
    C. Tight access administration, including for authorized 3rd parties.
    D. Diligent installation and patching of software applications.
    E. All of the above.
    F. None of the above

13. Management in your organization needs a demonstration of how well security policies, guidelines and procedures are implemented. Which of the following would be the optimal approach?
    A. Examine test results from the perspective of new and emerging threats.
    B. Assess test results based on the current threat landscape.
    C. Examine test results from a range of security tests.
    D. Conduct an independent evaluation for the policies, guidelines and procedures.

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

15. Which of the following is NOT a requirement for the design of an ISMS?
    A. The monitoring and review of the ISMS using measurements and audits.
    B. The definition and scope of an ISMS.
    C. The definition and application of a risk assessment process
    D. Identification of parties that are relevant and the understanding of their information security requirements.

PART II – Short Answer Questions (70 Marks)

1.	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.
2.	Information security versus usability: (10 Marks) A. Explain what you understand by information security? B. What do you understand by the term usability as it applies to IT systems? C. In what way does security affect usability? Give an example. D. In what way does usability affect security? Give example.
3.	Information security risk assessment takes into account threats, vulnerabilities and the impact. This is in addition to the probability that a particular threat would materialize in exploiting vulnerability. (12 marks) A. Define the terms threat, vulnerability and impact. B. Show relationship (if possible diagrammatically) among the three, i.e. threats, vulnerabilities and impact. C. In a 3x3 matrix, show the rating of risk given High, Medium and Low qualitative levels for impact and probability. Select one mitigation strategy and show how this strategy for a given risk; illustrate using the 3x3 matrix developed in the previous question.
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 technology components of an organization's security architecture.
5.	Organizations implement Information System Management Systems (ISMSs) as a means of protecting their information assets. (9 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. Name at least 4 steps of the seven steps in the ISMS implementation process.
6.	Information Security Audit (10 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 information security audit?

7.	Digital signatures: (10 marks) A. What are they? B. Show how cryptography implements digital signatures. C. Diagrammatically illustrate a digital signature system. D. Give examples of practical use of digital signatures.
8.	Security Administration (5 Marks) A. Explain what you understand by the term "security administration". B. Describe the role of tools used in security administration.
9.	Artificial Intelligence (AI) can be used to complement cyber security. (12 marks) A. Explain what you understand by Artificial Intelligence (AI); 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.
10.	The Internet of things (IoT) and Attack Surface: (12 Marks) A. Explain what you understand by the term 'attack surface" with respect to an organization or an information system. B. Why is 'attack surface' aggravated in IoT deployments? C. Explain (at least two) ways in which IoT security could be improved and hence address the challenge of attack surface. (4 marks)