JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR DIPLOMA IN CYBER SECURITY

2nd Year 1st SEMESTER 2024/2025 ACADEMIC YEAR

MAIN REGULAR

COURSE CODE: ISD 1204

COURSE TITLE: MANAGEMENT OF CYBER SECURITY

EXAM VENUE: **STREAM: (DIP. CYBER SECURITY)**

DATE: **EXAM SESSION: SEPT – DEC 2024**

TIME: 2.00 HOURS

Instructions:

This paper consists of two sections A and B

i. Attempt **ALL** questions in section A and any **THREE** in section B
ii. Candidates are advised not to write on the question paper.
iii. Candidates must hand in their answer booklets to the invigilator while in the examination room.

SECTION A

(Answer All questions in this section)

1. Define Cyber Security Risk Management and explain its significance in protecting an organization's information systems. (4 Marks)
2. Identify and explain the key concepts and terminologies involved in cyber security risk management. Include the terms: risk, asset, threat, vulnerability, and risk appetite. (5 Marks)
3. Why is creating an asset inventory important in establishing the risk context for cyber security? Provide examples of tangible and intangible assets. (4 Marks)
4. Describe how asset classification helps determine the protection required for different assets. Provide an example of classification. (4 Marks)
5. What factors should be considered when assessing an organization's risk appetite? (3 Marks)
6. Explain the role of employee security awareness in reducing cyber security risks. What are key areas to focus on? (4 Marks)
7. Define the terms: risk, threat, vulnerability, impact, and likelihood. Provide an example for each. (5 Marks)
8. What methodologies can organizations use to identify cyber security risks? Provide at least two techniques. (4 Marks)
9. How risks are assessed using a risk matrix? Provide an example of how to categorize risks as low, medium, and high. (4 Marks)
10. What role do vulnerability scanning tools play in identifying cyber security risks? Give an example of a tool. (3 Marks)

SECTION B

(Answer ANY THREE questions from this section)

11. (a) Define contingency planning in cyber security risk management. Explain the key components that make up an effective contingency plan. (10 Marks)

    (b) Explain the role of backup and recovery strategies in cyber security contingency planning. Discuss why regular testing of backup systems is critical. (10 Marks)

12. (a) What is a risk profile, and why is it important to monitor and update it regularly in cyber security risk management? (10 Marks)

(b) Discuss the role of automation in risk monitoring. Provide examples of automated tools used in continuous risk monitoring. (10 Marks)

13. (a) Describe the key components of a risk profile report. How should it be structured to effectively communicate the organization's risk posture to different stakeholders? (10 Marks)

    (b) Discuss the process of disseminating a risk profile report to relevant stakeholders. What methods can be used to ensure secure communication and proper documentation? (10 Marks)

14. (a) Discuss the role of a Security Operations Center (SOC) in monitoring and responding to cyber security threats. How do SOC analysts contribute to maintaining an organization's risk profile? (10 Marks)
    (b) Explain the process of preparing and disseminating risk profile reports to various stakeholders within an organization. Discuss how the reports should be tailored for different audiences (e.g., senior management, technical teams, and compliance officers). (10 Marks)