JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN IT SECURITY AND AUDIT

1st YEAR 1st SEMESTER 2024/2025 ACADEMIC YEAR

(KISUMU CAMPUS)

COURSE CODE : ICD 1108

COURSE TITLE : ADVANCED RISK MANAGEMENT IN INFORMATION ASSURANCE AND SECURITY

EXAM VENUE : STREAM : PhD

DATE :15/1/25 EXAM SESSION:14-17.00 HRS

TIME : 3.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE: COMPULSORY (20 MARKS)

a) Blockchain technology is emerging as a tool for enhancing data integrity and security. Discuss the role of blockchain in improving risk management practices, particularly within supply chain operations. **(7 Marks)**

b) The Internet of Things (IoT) introduces new cybersecurity risks due to the interconnection of devices. Explain the major cybersecurity risks associated with IoT devices and propose two strategies to mitigate these risks. **(7 Marks)**

c) Quantum computing is predicted to disrupt conventional encryption methods. Analyze the impact of quantum computing on existing encryption techniques and suggest ways organizations can prepare for post-quantum cryptography. **(6 Marks)**

QUESTION TWO: (20 MARKS)

a) Predictive analytics can enhance an organization's ability to manage cyber risks. Explain the role of predictive analytics in forecasting future cyber threats and discuss how it can be integrated into an organization's risk management framework. **(10 Marks)**

b) Discuss the vulnerability management challenges that organizations face in today's rapidly evolving threat landscape. Use the Equifax data breach (2017) as an example to illustrate your points. **(10 Marks)**

QUESTION THREE: (20MARKS)

a) The healthcare sector is a prime target for cybercriminals due to the sensitivity of patient data. Using the HIPAA regulation, discuss the best practices healthcare organizations should implement to protect patient information. **(10 Marks)**

b) Analyze the lessons learned from the Yahoo data breach in 2013-2014 and explain how organizations can improve their incident response strategies to avoid similar occurrences. **(10 Marks)**

QUESTION FOUR: (20MARKS)

a) National cybersecurity frameworks provide a structured approach to risk management. Compare and contrast the NIST Cybersecurity Framework (CSF) and ENISA's cybersecurity guidelines in terms of their risk management strategies. **(10 Marks)**

b) Supply chain attacks, such as the SolarWinds cyberattack (2020)**,** reveal vulnerabilities within third-party networks. Discuss how organizations can enhance supply chain security to mitigate risks arising from third-party vendors. **(10 Marks)**

QUESTION FIVE: (20 MARKS)

a) Emerging technologies like Artificial Intelligence (AI) and Machine Learning (ML) offer new tools for cybersecurity. Discuss the role of AI and ML in threat detection and how they can improve an organization's ability to respond to cyber threats. **(8 Marks)**

b) The SolarWinds cyberattack in 2020 was one of the most significant supply chain attacks in recent history. Hackers infiltrated the SolarWinds network management software and inserted malicious code into routine updates, which were then distributed to thousands of customers, including government agencies and corporations.

Task:

Based on the SolarWinds attack, discuss:

1. The vulnerabilities that enabled the attack to occur and spread across multiple organizations. **(4 Marks)**
2. How a well-developed supply chain risk management framework could have mitigated these risks. **(4 Marks)**
3. What lessons can be learned from this attack regarding third-party vendor security and incident response planning? **(4 Marks)**