JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE IN BACHELOR OF SCIENCE

COMPUTER SECURITY AND FORENSICS

3RD YEAR 2ND SEMESTER

2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB1304

COURSE TITLE: Computer Security Risk Management and Control

VENUE: LAB 5 **STREAM:**

DATE: 23/4/2025 **EXAM SESSION: 9.00-11.00**

TIME: 2.00 HOURS

INSTRUCTIONS:

---

1) **Answer QUESTION ONE (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**
4) **Mobile phones are NOT allowed in the examination room.**

QUESTION ONE (COMPULSORY) **(30 MARKS)**

a) Briefly explain four strategies for managing risk. (8 marks)

b) Explain why the Incident response policy needs to be explained to users and to be supported by Management (4 Marks)

c) Discuss any three kinds of computer security incidences that can face an organization like Safaricom. (6 marks)

d) What is the difference between proactive and reactive security measures? Provide examples of each. (6 marks)

e) Differentiate between threats, vulnerabilities, and risks in the context of cybersecurity. Provide an example for each. (6 Marks)

QUESTION 2 **(20 MARKS)**

a) Define risk management and outline the six steps in the risk management process (10 marks)

b) Explain how Disaster Recovery Planning (DRP) helps manage security risks in an organization. (10 marks)

QUESTION 3 **(20 MARKS)**

a) An organization experiences a data breach due to weak access controls. What **security control types** should be implemented to prevent future incidents? (10 marks)

b) Describe the containment, eradication, and recovery phases in incident response and their role in mitigating cyber threats. (10 marks)

QUESTION 4 **(20 MARKS)**

a) A company identifies a zero-day vulnerability in its network. What risk control measures should be applied to mitigate potential threats? (10 marks)

b) How can organizations apply **cost-benefit analysis** when selecting risk control measures? (10 marks)

QUESTION 5 **(20 MARKS)**

a) Explain the significance of the Protect function in the NIST Cybersecurity Framework. What security measures fall under this category? (10 Marks)

b) Explain the purpose of the "Recover" function in the NIST Cybersecurity Framework. Provide examples of recovery strategies that organizations can employ to minimize the impact of cybersecurity incidents. (10 Marks)

This is the last printed page