TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

Select department

UNIVERSITY EXAMINATION FOR:

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

CIS 4303: INFORMATION SECURITY AND RISK MANAGEMENT

END OF SEMESTER EXAMINATION

SERIES: December 2024

PAPER II

TIME:2HOURS

DATE: Pick DateSelect MonthPick Year

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of five questions. Attempt question ONE (Compulsory) and any other TWO questions.

Do not write on the question paper.

Question One

a) Define risk management and explain its importance in IT security (5 Marks)

b) Define the principles of confidentiality, integrity, and availability in information security (6 marks)

c) Outline the primary benefits of using a public-key encryption system (5 marks)

d) List the three main categories of security controls (3 Marks)

e) Explain how regular software and system updating mitigate security vulnerabilities (5 marks)

f) Differentiate between “risk avoidance” and “risk transference” in risk mitigation strategies (6 marks)

Question Two

a) information security review (6 Marks)

b) Outline two rules in segregation of duties as practiced in ICT security (4 marks)

c) Differentiate between:

i) Risk management and Risk Assessment (4 marks)

ii) Quantitative and Qualitative risk assessment. (6 Marks)

Question Three

a) Describe the purpose of auditing in information security management (3 marks)

Explain the role of cryptography in protecting data during transit and storage (6 Marks)

b) Explain how vulnerability analysis contributes to a robust IT risk management process (5 marks)

c) Identify three common types of human threats and their motivations. (6 Marks)

Question Four

a) Describe how organizations can use the risk-level matrix to prioritize and manage risks effectively (6 marks)

b) Explain the impact of human factors, such as employee awareness and training, on the overall security posture of an organization (6 Marks)

c) Describe how a cost-benefit analysis support decision-making during risk mitigation (8 marks)

Question Five

a) Discuss the ethical challenges faced by IT security professionals in managing sensitive data and preventing breaches (10 marks)

b) Create a checklist for testing an organization's business continuity plan (BCP) to ensure operational readiness during a disaster (10 Marks)