LAIKIPIA UNIVERSITY

UNIVERSITY EXAMINATIONS

FIRST SEMESTER 2025/2026 ACADEMIC YEAR

FOURTH YEAR EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION COMMUNICATION AND TECHNOLOGY

BICT 412: INFORMATION SECURITY AUDIT AND ASSURANCE

STREAM: R ***TIME: 2 HRS***

DAY: MONDAY [8.30 – 10.30 A.M] ***DATE: 02/02/2026***

THIS QUESTION PAPER CONSISTS OF THREE (3) PAGES

PLEASE DO NOT OPEN UNTIL THE INVIGILATOR SAYS SO.

INSTRUCTIONS: Section A is compulsory and has **30 marks.**

Attempt any **TWO** questions from Section **B**. Each question has **20 marks.**

SECTION A – 30 MARKS (ANSWER ALL QUESTIONS)

QUESTION ONE (30 MARKS)

(a) What is information security governance? Who in the organization should plan for it? **(2 Marks)**

(b) Discuss the changing role of an IS auditor in a computerized environment **(2 Marks)**

(c) Describe the critical characteristics of information. How are they used in the study of computer security? **(3 Marks)**

(d) Why is the top-down approach to information security superior to the bottom-up approach? **(3 Marks)**

(e) Why is a methodology important in the implementation of information security? How does a methodology improve the process? **(4 Marks)**

(f) What are the three general categories of unethical and illegal behaviour? **(3 Marks)**

(g) Discuss at least **TWO** sampling methods available to IS auditors **(4 Marks)**

(h) In risk management strategies, why must periodic review be a part of the process? **(3 Marks**

(i) What is risk assessment? Write about the five variables, used for risk assessment **(6 Marks)**

SECTION B – 40 MARKS (ANSWER ANY TWO QUESTIONS)

QUESTION TWO

(a) Why is information security a management problem? What can management do that technology cannot? **(3 Marks)**

(b) Why do employees constitute one of the greatest threats to information security? **(3 Marks)**

(c) What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms? **(4 Marks)**

(d) Why does polymorphism cause greater concern than traditional malware? How does it affect detection? **(4 Marks)**

(e) What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why? **(6 Marks)**

QUESTION THREE

(a) What is risk management? Why is the identification of risks, by listing assets and their vulnerabilities, so important to the risk management process? **(4 Marks)**

(b) Briefly discuss why networking components need more examination from an information security perspective than from a systems development perspective? **(4 Marks)**

(c) How can a security framework assist in the design and implementation of a security infrastructure? **(3 Marks)**

(d) What Web resources can aid an organization in developing best practices as part of a security framework? **(3 Marks)**

(e) . Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework **(6 Marks)**

QUESTION FOUR

(a) What are the knowledge requirements for an IS auditor and what are the sources for such knowledge? **(4 Marks)**

(b) What is audit evidence? What are the important points that IS Auditors need to remember while for collecting and evaluating evidence **(4 Marks)**

(c) What are Computer Assisted audit Tools and Techniques (CAATTs)? Describe the types of CAATTs and their usefulness to IS auditors. **(6 Marks)**

(d) What is impact analysis from the risk assessment point of view? Discuss in detail with the help of a risk-level matrix **(6 Marks)**

QUESTION FIVE

(a) Why do organizations need to implement ISMS? Discuss at least **FOUR** benefits of ISMS to organizations. **(6 Marks)**

(b) Discuss the **FOUR** key components of an ISMS **(8 Marks)**

(c) Elaborate in details the steps involved in implementing an ISMS **(6 Marks)**