MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2023/2024

THIRD YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR
OF COMPUTER SECURITY AND FORENSICS

CCF 3450: INFORMATION SYSTEMS AUDIT

DATE: APRIL 2024   **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a. Explain any three tools that can be used to identify vulnerabilities   (6 marks)

b. Categorize the various types of audits   (5 marks)

c. What is COBIT? Give three reasons why an organization should adopt COBIT.
                                                                                                                  (5 Marks)
d. Distinguish between internal controls and external controls   (2 marks)

e. An ERP application seeks to do away with this fragmented approach to the business
    information management by integrating diverse functions which exchange
    information between them. The main purpose of an ERP system is to facilitate the
    flow of information between all business functions within an organization and

manage the connections with external stakeholders. Outline any six Audit related

questions concerning ERP systems. (6 marks)

f. Briefly describe three strategies for managing risk. (6 marks)

QUESTION TWO (20 MARKS)

XYZ Electronics Ltd. is a company specializing in the manufacturing of electronic devices. As an auditor, you have been engaged to conduct the information systems audit of XYZ Electronics Ltd.

Required

a. Using a diagram illustrate the stages of the audit process that you would engage in

during the process of doing the audit. (5 marks)

b. Explain any five techniques you would use to gather evidence during the audit

(5 marks)

c. Explain any five types of audit risks you would look at. (5 marks)

d. Explain any five advantages of using computer assisted audit techniques (CAATS)in the process (5 marks)

QUESTION THREE (20 MARKS)

For an organization to ensure secure operations of information systems and thus safeguard assets and the data stored in these systems, and to ensure that applications achieve their objectives in an efficient manner, an organization needs to institute a set of policies, procedures, and technological measures, collectively called systems controls.

Required

a. Explain the objectives of system control (5 marks)

b. Explain types of security controls (5 marks)

c. As an auditor explain, how audit trails can be used to support security objectives in

the organization (10 marks).

QUESTION FOUR (20 MARKS)

Suppose you have been employed as an information system auditor for Ngundune bank where you have been included in a team responsible for initiating a business continuity and disaster recovery plan. The manager of the bank has tasked you in the development of a disaster recovery plan.

Required

    i.   Discuss the steps of coming up with a disaster recovery plan.   (6 marks)

    ii.   In implementing the systems or capabilities required to deliver the plan, there are three primary types of sites to deal with situations where the data center or main facility are unavailable. Describe these three types of site.   (6 marks)

    iii.   Is business continuity the same as disaster recovery planning? Discuss your answer   (4 marks)

    iv.   iv. Explain how you can audit business continuity.   (4 marks)

QUESTION FIVE (20 MARKS)

a) An information technology security policy is a set of rules, guidelines, and procedures that outline how an organization should manage, protect, and distribute its information assets. The policy aims to reduce the risk of data breaches, unauthorized access, and other security threats by providing a structured approach to information security management. Discuss the key elements of an IT security policy   (10 marks).

b) The framework for the ISACA IS auditing standards provides for multiple levels, as follows: procedures, standards and guidelines. Describe each of the above and give one example of each   (10 marks)