



TECHNICAL UNIVERSITY OF MOMBASA

Select Faculty/School/Institute

Select department

UNIVERSITY EXAMINATION FOR:

BSC I.T

BIT 2318: INFORMATION SYSTEM AUDIT

SPECIAL SUPPLEMENTARY EXAMINATION

SERIES: APRIL 2017

TIME: 2 HOURS

DATE: 10 Sep 2017

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of Choose No questions. Attempt Choose instruction.

Do not write on the question paper.

Question ONE

- a) Discuss any three issues that should be considered by a system auditor at post implementation review stage before preparing the audit report. (6 Marks)
- b) Explain the following terms with reference to Information Systems Audit (4 Marks)
- (i) Risk
 - (ii) Threat
 - (iii) Vulnerability
 - (iv) Exposure
- b) As an information system auditor explain how you can use the COBIT framework as a guide when auditing an organisation. (4 Marks)
- ii) Discuss any three areas that are to be explored to determine risks in IT Company. (6 Marks)
- c) State and explain four commonly used techniques to assess and evaluate risks in an enterprise. (8 Marks)
- d) Suggest any two procedural plans for disaster recovery. (2 Marks)

Question TWO

Q2

a) Lovely Solutions has recently developed a core banking application software for the Real Bank Limited (RBL) which has more than sixty branches. One of the main distinguishing features of the new system is that it is able to provide online connectivity to all branches. Prior to implementing the application, management of RBL wants to know the measures taken by the Lovely Solutions for ensuring the availability of the system when multiple users will access it simultaneously. The management is also concerned about the change over strategies that can be adopted for replacing the existing system and the associated risks which may be faced during change over process.

i) Identify tests performed by Lovely Solutions to ensure that the system will remain available and its efficiency will not be compromised on account of simultaneous log in by a number of users. **(6 Marks)**

ii) List three major steps involved in change over from old to new system. **(3 Marks)**

iii) The risks which the management may face during the change over process. **(6 Marks)**

b) As an information system auditor explain how you can use the Certified Information Systems Auditor (CISA) framework as a guide when auditing an organisation. **(5 Marks)**

Question THREE

Q3 The CEO of Pombe Securities & Exchange Company is concerned about the rising number of frauds being reported in the industry specially those carried out by insiders. Recently another financial institution in the same region had suffered a loss of Sh. 10 million due to a fraud which was committed by a senior executive who was responsible for carrying out a number of key responsibilities related to information systems. The CEO has requested you to advise the company on prevention and detection measures against such threats to their information systems.

i) Discuss the principle of tying duties to employees in relation to fraud **(10 Marks)**

ii) Suggest best practices for preventing and detecting frauds that may be committed by key information systems personnel. **(10 Marks)**

Question FOUR

(a) The risk management process involves the identification and classification of assets and assessing the

threats associated with the identified assets,

- i) identify four types of information assets associated with information technology
(4 Marks)
- ii) Explain threats associated with each asset and The possible impact of the identified threats.
(16 Marks)

Question FIVE

a)After a recent security breach of information systems in Mamboleo Enterprises, an emergency meeting was called by Board of Directors of the company in which members of executive management, steering committee and chief information security officer also participated. Unfortunately, instead of finding the root cause of security breach and determining future course of action for managing various risks to which the organization may be exposed to, the meeting was marred by finger-pointing.

- i) List major steps for a ‘security incident handling and response’ mechanism in an organization. (7 Marks)
- ii) Identify at least **two** important responsibilities related to “Risk Management”, for each of the following:
 - a. Board of directors
 - b. Steering committee
 - c. Executive Management(6Marks)

- b) Explain audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order. (7 Marks)