namibia university
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Computer Science

QUALIFICATION: Bachelor of Computer Science	
QUALIFICATION CODE: 07BACS	**LEVEL: 6**
COURSE: Systems Audit	**COURSE CODE:** SAU620S
DATE: January 2023	**SESSION:** 2
DURATION: 2 hours 30 minutes	**MARKS:** 60

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MS HELENA HAINANA**
MODERATOR:	**DR MERCY CHITAURO**

THIS QUESTION PAPER CONSISTS OF 3 PAGES

(Including this front page)

INSTRUCTIONS:

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions you should be guided by the allocation of marks. Do not give too few or too many facts in your answers.

1. Introduction to Systems Audit   [10 Marks]

a) Briefly explain the five major components of an information system that an auditor would need to focus on.

2. IT Audit Process: Technology and audit [10 Marks]

As the IT audit senior of the engagement, you are presenting to the IT manager and partner (as part of the planning meeting) the results of the risk assessment performed.

a) What is an audit universe and what does it include in the context of NTI? [4]

b) Three types of risk are normally considered when using a risk-based audit approach. Briefly describe these three types of risks. [6]

3. Standards and Guidelines for IS auditing [9 Marks]

a) The IIA standards have been regrouped and redefined into attribute, performance, and implementation standards. Briefly state the key focus of each of these groups. [6]

b) The framework for the IT auditing standards provides multiple levels of guidance, that is, standards, guidelines and procedures. Briefly define the three levels. [3]

4. Information systems/information technology governance [6 Marks]

a). CoCo is an Audit body Intended to translate COSO controls into practical, implementable activities. State four ways in which CoCo promotes the treatment of IS risks. [4 Marks]

b) The Payment Card Industry Security Standards Council developed a set of standards to encourage cardholder data security and facilitate the adoption of consistent data security measures on a global basis. State two directives defined by the standard. [2 Marks]

5. Audit and development of application controls [5 Marks]

a) State the importance of Audit trails in IS Auditing. [1 Mark]

b) Each database in IDEA has several properties associated with it; which is accessible from the Properties window. List and explain one property of your choice. [2 Marks]

c) What are some of the problems associated with the use of CAATS? [2 Marks]

6. Information Technology Service Delivery and Support. [6 Marks]

a) Continuous monitoring is seen as a key activity in assessing the security impacts on an information system resulting from planned and unplanned changes. List the six steps for the continuous monitoring framework. [3]

b) Define change control and state its' core objective. [3 Marks]

7. Auditing UNIX and Windows. [4 Marks]

a) Give one example of a UNIX daemon. [1 Mark]

b) Define password shadowing and state the benefit of implementing it. [3 Marks]

8. Investigating IT fraud [10 Marks]

a) Mandia and Prosise define an incident response methodology incorporating 9 stages. List the 9 stages of incidence response methodology. [7 Marks]

b) In relation to IS Auditing, state three reasons why cyber fraud prosecution fails? [3 Marks]

[THE END]