NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Computer Science Department

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE (SYSTEMS ADMINISTRATION)	
QUALIFICATION CODE: 07BACS	**LEVEL:** 6
COURSE: SYSTEMS AUDIT	**COURSE CODE:** SAU620S
DATE: NOVEMBER 2019	**PAPER:** THEORY
DURATION: 2 Hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION MEMORANDUM	
EXAMINER(S)	Mr Munyaradzi Maravanyika
MODERATOR:	Mrs Mercy Chitauro

INSTRUCTIONS
1. Please use the memorandum or sample solutions to guide your marking. 2. Use the marks allocated as a guide to mark 3. Reasonable, in depth and innovative correct solutions provided by the students should be allocated marks even if not provided in the memorandum. 4. Take note of the marks allocated to each question.

PERMISSIBLE MATERIALS

None

THIS QUESTION PAPER CONSISTS OF 6 PAGES
(Including this front page)

1. **Introduction to Systems Audit** **[10 Marks]**

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

Computer hardware	*This is the physical technology that works with information. Hardware can be as small as a smartphone that fits in a pocket or as large as a supercomputer that fills a building. Hardware also includes the peripheral devices that work with computers, such as keyboards, external disk drives, and routers. With the rise of the Internet of things, in which anything from home appliances to cars to clothes will be able to receive and transmit data, sensors that interact with computers are permeating the human environment.*	*2*
Computer Software	*The hardware needs to know what to do, and that is the role of software. Software can be divided into two types: system software and application software. The primary piece of system software is the operating system, such as Windows or iOS, which manages the hardware's operation. Application software is designed for specific tasks, such as handling a spreadsheet, creating a document, or designing a Web page.*	*2*
Telecommunications	*This component connects the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibre optics, or wireless, such as through Wi-Fi. A network can be designed to tie together computers in a specific area, such as an office or a school, through a local area network (LAN). If computers are more dispersed, the network is called a wide area network (WAN). The Internet itself can be considered a network of networks.*	*2*
Databases and data warehouses	*This component is where the "material" that the other components work with resides. A database is a place where data is collected and from which it can be retrieved by querying it using one or more specific criteria. A data warehouse contains all of the data in whatever form that an organization needs. Databases and data warehouses have assumed even greater importance in information systems with the emergence of "big data," a term for the truly massive amounts of data that can be collected and analyzed*	*2*

Human resources and procedures	*The final, and possibly most important, component of information systems is the human element: the people that are needed to run the system and the procedures they follow so that the knowledge in the huge databases and data warehouses can be turned into learning that can interpret what has happened in the past and guide future action*	*2*

2. IT Audit Process: IT Audit Function Knowledge [15]

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]

• *The audit universe is, first and foremost, a living document that has to be updated on a periodic basis.* • *It should capture all of the businesses, regions and functions that make up the organization.* • *There has to be collaboration between key business stakeholders and internal audit to come up with this audit universe, but it should be primarily driven by the audit function.* • *Upon creation of this audit universe, there is a means to perform the risk assessment, which is primarily an enterprise risk-level activity.*	*4*

b. Three types of risk are normally considered when using a risk-based audit approach. Briefly describe these three types of risks. [11]

• *Inherent Risk*	• *Inherent risk is the likelihood of a significant loss occurring before taking into account any risk-reducing factors.* • *In evaluating inherent risk, the auditor must consider what are the types of and nature of risks as well as what factors indicate a risk exists.* • *To achieve this the auditor must be familiar with the environment in which the entity operates.*	*3*
• *Control Risk*	• *Control risk measures the likelihood that the control processes established to limit or manage inherent risk are ineffective.* • *In order to ensure that internal audit evaluates the controls properly, the auditor must understand how to measure which controls are effective.*	*4*

	• *This will involve identifying those controls that provide the greatest degree of assurance to inimize risks within the business.* • *Control effectiveness is strongly impacted by the quality of work and control supervision.* • *Controls in business operations provide the major line of defense against inherent risk.* • *In general, the auditor may assume that stronger controls reduce the amount of risk; however, at some point the cost of control may become prohibitive (in terms of both monetary and staff resources as well as customer satisfaction).* ***[Any 4]***	
• *Audit Risk*	• *Audit risk is the risk that audit coverage will not address significant business exposures.* • *Pro-forma audit programs may be developed in order to reduce audit risk.* • *These provide guidance as to which key controls should exist to address the risk, and the recommended compliance and/or substantive test steps to be performed.* • *These programs should be used with care and modified to reflect the current business risk profile.*	*4*

3. Standards and Guidelines for IS auditing **[15]**

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]

Attribute Standards.	*These address the attributes of organizations and individuals performing internal audit services and apply to all internal audit services.*	*2*
Performance Standards.	*These describe the nature of internal audit services provided and provide quality criteria against which the performance of these services can be measured.*	*2*
Implementation Standards.	*These prescribe Standards applicable to specific types of engagements in a variety of industries as well as specialist areas of service delivery.*	*2*

b. The framework for the IT auditing standards provides multiple levels of guidance, that is, standards, guidelines and procedures. Briefly discuss the three levels. [9]

Standards	*Define mandatory requirements for IT auditing and reporting. They inform:* • *IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IT auditors* • *Management and other interested parties of the profession's expectations concerning the work of practitioners* • *Holders of the Certified Information Systems Auditor designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action*	*3*
Guidelines	• *Guidelines provide guidance in applying IT auditing standards.* • *The IT auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application, and be prepared to justify any departure.* • *The objective of the IT auditing guidelines is to provide further information on how to comply with the IT auditing standards.*	*3*
Procedures	• *Procedures provide examples of procedures an IT auditor might follow in an audit engagement.* • *The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements.* • *The objective of the IT auditing procedures is to provide further information on how to comply with the IT auditing standards.*	*3*

4. Information systems/information technology governance **[10]**

Three standards have become widely recognized as *IT governance* frameworks. While each has significant IT governance strengths, none may be looked on as a complete IT governance solution. Outline the major components of the ITIL, COBIT and ISO/IEC 38508 frameworks.

ISO/IEC 38508	*The framework sets out six principles for good orporate governance of IT under the headings of:* *1. Responsibility* *2. Strategy* *3. Acquisition* *4. Performance* *5. Conformance* *6. Human behaviour* ***[Any 4]***	*4*
COBIT	*CobiT regards IT governance as a balance between two primary areas:* *1. Creation of corporate value* *2. Minimizing IT risks* *With overall objectives of:* • *Ensuring strategic orientation, focusing on corporate solutions.* • *Creation of benefits, focusing on optimizing the tasks and assessing the benefit of the IT.* • *Implementation of risk management relating to the protection of the* • *IT assets and taking account of disaster recovery and continuation of the corporate processes in the event of a crisis.* • *Effective resource management in order to ensure the optimization of knowledge and infrastructure.* • *Adequacy of performance measurement and the creation of the bases for continual improvement.* ***[Any 4]***	*4*
ITIL	*Although it is directed specifically toward service management, a part of that is, itself, directed toward the governance of service delivery.*	*2*

5. Audit and development of application controls **[20]**

Explain the control objectives for each stage of the SDLC.

Methodology	• *Formalized, structured methodology will be followed* • *Roles and responsibilities will be clearly laid out and adhered to* • *Methodology will be kept up to date and in step with current developments* ***[Any 2]***	*2*
Project Initiation	• *Each new project will be clearly scoped prior to commencement of work* • *The user department will be involved in the definition and authorization of new or modified systems* • *Team assignments will result in the use of appropriately skilled and qualified staff* • *Commencement of each phase will be preceded by the appropriate authorization* ***[Any 3]***	*3*
Feasibility Study	• *Alternative courses of action will be evaluated in order that an appropriate solution be selected* • *Technological feasibility of the recommended solution will be assured* • *All relevant costs will be included in the cost/benefit analysis* • *All relevant risks will have been identified and quantified* • *Project approval will be given by the appropriate management based on knowledge* • *Project will be capable of being monitored through its existence* ***[Any 2]***	*2*
Systems Design	• *Design methodology is appropriate to the proposed system (Life cycle,*	*4*

	Structured, Database, Skeletal, Prototype) • *Documentation will be created to standard Input validation requirements will be appropriate* • *File structures will be as per departmental standards* • *All requisite processing steps will be identified and designed into the system* • *All programs will be fully specified as per departmental standards* • *All sources of data required for the system will be identified and approved* • *Security requirements of the system will be fully defined and approved* • *Audit trails will be appropriate and approved* • *Documentation of the system design will adhere to departmental standards* • *Overall design shall include the design of appropriate testing and verification plans* • *Design approval will be obtained from the appropriate levels of management*	
Development and Implementation	• *Written narratives of all programs in the system will be available and up to date* • *Commercial packages selected will be compatible with existing operations and departmental policies* • *Use of contracted programming staff will be approved and the quality of their work will be contracted for* • *Operational documentation will be produced according to departmental standards* • *Training plans will be produced for all users of the system* • *Program testing will be comprehensive and effective* ***[Any 4]***	*4*

	• *System testing will test both for functional capability as well as operational efficiency* • *Conversion planning will ensure smooth conversion to the new system* • *Acceptance testing will be comprehensive and carried out by the appropriate staff*	
System Operations	• *All organizational controls will operate as designed and intended* • *Cost monitoring will ensure efficient operation of the system* • *Modifications to the system will only be permitted via the departmentally authorized route*	*3*

6. Impact of Information Technology on the Business Processes and Solutions [6]

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.

Step 1. Categorization of Information System *Step 2. Selection of Security Controls* *Step 3. Implementation of Security Controls* *Step 4. Assessment of Security Controls* *Step 5. Authorization of Information Systems* *Step 6. Monitoring of Security Controls*	*6*

7. Auditing UNIX and Windows. [4]

a. Give any two examples of UNIX daemons. [1]

b. Give three aspects the systems administrator should check for problem areas on a random basis [3]

8. Investigating IT fraud [20]

Mandia and Prosise define an incident response methodology as incorporating, among others:

1. Pre-incident preparation
2. Detection of incidents
3. Initial response
4. Duplication (forensic backups)
5. Investigation
6. Network monitoring

7. Recovery
8. Reporting
9. Follow-up

Briefly describe each of these stages of incidence response methodology.

Pre-incident preparation	*The objectives of pre-incident preparation are to ensure that, should an incident occur, the organization is in a position to identify what exactly happened and to what systems.*	*2*
Detection of incidents	*Incidents may be detected via IDS, firewalls, suspicious account activity, malfunctioning services, or even defaced web sites*	*2*
Initial response	*The initial response should be directed toward determining what probably happened and determining what is the best response strategy. At all times the investigator must be mindful of the legalities and must ensure that all searches are carried out within the letter of the law.*	*2*
Duplication (forensic backups)	*Forensic examinations should never be performed on the original media. An exact clone of the media should be made and the original evidence must then be stored securely. Care must be taken to ensure that the cloned media is in fact a complete copy of the original evidence*	*3*
Investigation	*Once a working copy of the data is available, the investigator must decide what evidence is to be sought*	*2*
Network monitoring	*In the course of the investigation of an ongoing fraud, the investigator may have to monitor traffic flowing over the communication network. This will typically involve using packet sniffers to monitor traffic flow. Such activity is purely detective and is designed to confirm or dispel suspicions*	*3*
Recovery	*Recovery involves the restoration of the computer systems to an acceptable security level and may involve resorting to backups, hardening of the operating environment, and increased user education*	*2*
Reporting	*Reporting may be external or internal. External reporting is typically intended to support criminal actions against perpetrators. Internal reporting is*	*2*

	generally intended to communicate lessons learned and amendments required to prevent repetitive incidents.	
Follow-up	*Follow-up is a prerequisite in order to ensure action, external or internal, has been taken and will be effective. It should be noted by the auditor that follow-up does not involve a repeat of the audit. Where recommendations have been made and security remedies have been selected, the follow-up is a measurement of the effectiveness of their implementation and utilization, including the ongoing monitoring of vulnerabilities.*	*2*

END OF MEMORANDUM