NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Informatics

QUALIFICATION : BACHELOR OF INFORMATICS HONOURS (BUSINESS INFORMATICS)	
QUALIFICATION CODE: 08BIH	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE NAME:** INFORMATION SYSTEMS AUDIT
DATE: JANUARY 2020	**PAPER: THEORY**
DURATION: 3 Hours	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR MUNYARADZI MARAVANYIKA
MODERATOR:	MR PANDULENI NDILULA

INSTRUCTIONS
1. Answer ALL the questions. 2. Write clearly and neatly. 3. Number the answers clearly. 4. Do not use additional materials 5. Cross out any work which should not be marked. 6. No pencil work allowed except for diagrams where requested.

THIS QUESTION PAPER CONSISTS OF 1 PAGE
(Excluding this front page)

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

a. The framework for the ISACA IS Audit and Assurance Standards provides for multiple levels of documents, such as standards, guidelines, and tools and techniques. Distinguish between standards, guidelines, and tools and techniques. [5]

b. There are three categories of standards and guidelines—general, performance and reporting. Briefly describe the main focus of each of these categories. [5]

2. IT Audit Process: Technology and audit **[20 Marks]**

An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit programs. Although an audit program does not necessarily follow a specific set of steps, the IS auditor typically would follow, as a minimum course of action, sequential program steps to gain an understanding of the entity under audit, evaluate the control structure and test the controls. Outline the steps an auditor would typically follow and what each one entails.

3. Information Technology Governance and Management **[20 Marks]**

Strategic planning from an IS standpoint relates to the long-term direction an enterprise wants to take in leveraging IT for improving its business processes. Briefly discuss strategic planning from an Information Systems Auditor's perspective.

4. Information Systems Acquisition, Development and Implementation **[10 marks]**

The IS auditor's tasks in system development, acquisition and maintenance may take place once the project is finished or during the project itself. Most tasks in the following list cover both scenarios and the IS auditor is expected to determine which task applies. Discuss the typical tasks an IS Auditor is expected to conduct during systems development, acquisition and maintenance.

5. Information Systems Operations, Maintenance and Service Management **[20 Marks]**

The IS auditor should review controls over network implementations to ensure that standards are in place for designing and selecting a network architecture, and for ensuring that the costs of procuring and operating the network do not exceed the benefits. Discuss the issues an IS Auditor must consider when reviewing network implementations.

6. Protection of Information Assets **[20 Marks]**

An information security management system (ISMS) is a framework of policies, procedures, guidelines and associated resources to establish, implement, operate, monitor, review, maintain and improve information security for all types of organizations. An ISMS is defined in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series of standards and guidelines. Describes the related key elements of information security management.

End of question paper

Moderated

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Informatics

QUALIFICATION : BACHELOR OF INFORMATICS HONOURS (BUSINESS INFORMATICS)	
QUALIFICATION CODE: 08BIH	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE NAME:** INFORMATION SYSTEMS AUDIT
DATE: JANUARY 2020	**PAPER: THEORY**
DURATION: 3 Hours	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR MUNYARADZI MARAVANYIKA
MODERATOR:	MR PANDULENI NDILULA

INSTRUCTIONS
1. Answer ALL the questions. 2. Write clearly and neatly. 3. Number the answers clearly. 4. Do not use additional materials 5. Cross out any work which should not be marked. 6. No pencil work allowed except for diagrams where requested.

THIS QUESTION PAPER CONSISTS OF 1 PAGE
(Excluding this front page)

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Informatics

QUALIFICATION : BACHELOR OF INFORMATICS HONOURS (BUSINESS INFORMATICS)	
QUALIFICATION CODE: 08BIH	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE NAME:** INFORMATION SYSTEMS AUDIT
DATE: JANUARY 2020	**PAPER: THEORY**
DURATION: 3 Hours	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION MEMORANDUM	
EXAMINER(S)	MR MUNYARADZI MARAVANYIKA
MODERATOR:	MR PANDULENI NDILULA

THIS QUESTION PAPER CONSISTS OF 10 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. Do not use additional materials
5. Cross out any work which should not be marked.
6. No pencil work allowed except for diagrams where requested.

1. Introduction to Systems Audit [10 Marks]

a. The framework for the ISACA IS Audit and Assurance Standards provides for multiple levels of documents, such as standards, guidelines, and tools and techniques. Distinguish between standards, guidelines, and tools and techniques. [5]

• *Standards define mandatory requirements for IS audit and assurance and reporting.*	*1*
• *Guidelines provide guidance in applying IS Audit and Assurance Standards.* • *The IS auditor should consider them in determining how to achieve implementation of the above standards, use professional judgment in their application and be prepared to justify any departure from the standards.*	*2*
• *Tools and techniques provide examples of processes an IS auditor might follow in an audit engagement.* • *The tools and techniques documents provide information on how to meet the standards when completing IS auditing work, but do not set requirements.*	*2*

b. There are three categories of standards and guidelines—general, performance and reporting. Briefly describe the main focus of each of these categories. [5]

***General**—The guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.*	*2*
***Performance**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care*	*2*
***Reporting**—Address the types of reports, means of communication and the information communicated*	*1*

2. IT Audit Process: Technology and audit [20 Marks]

An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit programs. Although an audit program does not necessarily follow a specific set of steps, the IS auditor typically would follow, as a minimum course of action, sequential program steps to gain an understanding of the entity under audit, evaluate the control structure and test the controls. Outline the steps an auditor would typically follow and what each one entails.

Audit Phase	***Description***	
Audit subject	• *Identify the area to be audited.*	*2*
Audit objective	• *Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.*	*2*
Audit scope	• *Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.*	*2*
Preaudit planning	• *Identify technical skills and resources needed.* • *Identify the sources of information for test or review such as functional flow charts, policies, standards, procedures and prior audit work papers.* • *Identify locations or facilities to be audited.* • *Develop a communication plan at the beginning of each engagement that describes who to communicate to, when, how often and for what purpose(s).*	*3*
Audit procedures and steps for data gathering	• *Identify and select the audit approach to verify and test the controls.* • *Identify a list of individuals to interview.* • *Identify and obtain departmental policies, standards and guidelines for review.* • *Develop audit tools and methodology to test and verify control.*	*3*
Procedures for evaluating the test or review results	• *Identify methods (including tools) to perform the evaluation.* • *Identify criteria for evaluating the test (similar to a test script for the auditor to use in conducting the evaluation).* • *Identify means and resources to confirm the evaluation was accurate (and repeatable, if applicable).*	*3*
Procedures for communication with management	• *Determine frequency of communication.* • *Prepare documentation for final report.*	*2*

Audit report preparation	• *Disclose follow-up review procedures.* • *Disclose procedures to evaluate/test operational efficiency and effectiveness.* • *Disclose procedures to test controls.* • *Review and evaluate the soundness of documents, policies and procedures.*	*3*

Information Technology Governance and Management **[20 Marks]**

Strategic planning from an IS standpoint relates to the long-term direction an enterprise wants to take in leveraging IT for improving its business processes. Briefly discuss strategic planning from an Information Systems Auditor's perspective.

• *Under the responsibility of top management*
• *Factors to consider include:*
  o *identifying cost effective IT solutions in addressing problems*
  o *opportunities that confront the enterprise, and*
  o *developing action plans for identifying and acquiring needed resources.*
• *In developing strategic plans, generally three to five years in duration, enterprises should ensure that the plans are fully aligned and consistent with the overall organizational goals and objectives.*
• *IT department management, along with the IT steering committee and the strategy committee (which provides valuable strategic input related to stakeholder value), play a key role in the development and implementation of the plans.*
• *Effective IS strategic planning involves a consideration of the enterprise's requirements for new and revised IS systems and the IT organization's capacity to deliver new functionality through well-governed projects.*
• *Determining requirements for new and revised IS systems will involve a systematic consideration of the enterprise's strategic intentions, how these translate into specific*
• *objectives and business initiatives, and what IT capabilities will be needed to support these objectives and initiatives.*
• *In assessing IT capabilities, the existing system's portfolio should be reviewed in terms of functional fit, cost and risk.*
• *Assessing IT's capacity to deliver involves a review of the organization's technical IT infrastructure and key support processes (e.g., project management, software development and maintenance practices, security administration and help desk services) to determine whether expansion or improvement is necessary.*	

• *It is important that the strategic planning process encompasses the delivery of new systems and technology and considers return on investment (ROI) on existing IT and the decommissioning of legacy systems.* • *The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support the business strategies.* • *The IS auditor should pay full attention to the importance of IS strategic planning, taking management control practices into consideration.* • *In addition, the IT governance objective requires that IT strategic plans be synchronized with the overall business strategy.* • *An IS auditor must focus on the importance of a strategic planning process or planning framework.* • *Particular attention should be paid to the need to assess how operational, tactical or business development plans from the business are taken into account in IT strategy formulation, contents of strategic plans, requirements for updating and communicating plans, and monitoring and evaluation requirements.* • *The IS auditor should consider how the CIO or senior IT management are involved in the creation of the overall business strategy.* • *A lack of involvement of IT in the creation of the business strategy indicates that there is a risk that the IT strategy and plans will not be aligned with the business strategy.*	
Allocate 2 marks for each correct bullet point [max 10 points]	

4. Information Systems Acquisition, Development and Implementation [10 marks]

The IS auditor's tasks in system development, acquisition and maintenance may take place once the project is finished or during the project itself. Most tasks in the following list cover both scenarios and the IS auditor is expected to determine which task applies. Discuss the typical tasks an IS Auditor is expected to conduct during systems development, acquisition and maintenance.

• *Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.* • *Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risks to and exposures of the system.* • *Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risks to and exposures of the system.* • *Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementation of controls.* • *Periodically meet with systems development and user project team members, and review the documentation and deliverables to monitor the systems development process to ensure that controls are implemented, user and*	

business requirements are met, and the systems development/acquisition methodology is being followed. • *Also review and evaluate the application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls.* • *Audit trails are tracking mechanisms that can help IS auditors ensure program change accountability. Tracking information in a change management system includes:* – *History of all work order activity (date of work order, programmer assigned, changes made and date closed)* – *History of logons and logoffs by programmers* – *History of program deletions* – *Adequacy of SoD and quality assurance activities* • *Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources.* • *Participate in postimplementation reviews.* • *Review and analyse test plans to determine if defined system requirements are being verified.* • *Analyse test results and other audit evidence to evaluate the system maintenance process to determine whether control objectives were achieved.* • *Review appropriate documentation, discuss with key personnel and use observation to evaluate system maintenance standards and procedures to ensure their adequacy.* • *Discuss and examine supporting records to test system maintenance procedures to ensure that they are being applied as described in the standards.*	
Allocate 1 marks for each correct bullet point [max 10 points]	

5. Information Systems Operations, Maintenance and Service Management [20 Marks]

The IS auditor should review controls over network implementations to ensure that standards are in place for designing and selecting a network architecture, and for ensuring that the costs of procuring and operating the network do not exceed the benefits. Discuss the issues an IS Auditor must consider when reviewing network implementations.

Physical Controls		
• *Network hardware devices* • *File server* • *Documentation*	• *Are network hardware devices located in a secure facility and restricted to the network administrator?* • *Is the housing of network file servers locked or otherwise secured to prevent removal of boards, chips or the computer itself?* • *Is the device tagged where appropriate?*	*2*
• *Key logs*	• *Are the keys to the network file server facilities controlled to prevent the risk of unauthorized access?*	*2*

	• *Are keys assigned only to the appropriate people (e.g., the network administrator and support staff)?* • *Select a sample of keys held by people without authorized access to the network file server facilities and wiring closet in order to determine that these keys do not permit access to these facilities.*	
• *Network wiring closet and transmission wiring*	• *Is the wiring physically secured?* • *Is the wiring labeled where appropriate?*	*2*
Environmental controls		
• *Server facility*	• *Are temperature and humidity controls adequate?* • *Have static electricity guards been put in place?* • *Have electric surge protectors been put in place?* • *Has a fire suppression system been put in place and is it tested/inspected regularly?* • *Are fire extinguishers located nearby and inspected regularly?* • *Are the main network components equipped with an uninterruptible power supply* • *(UPS) that will allow the network to operate in case of minor power fluctuations or to be brought down gracefully in case of a prolonged power outage?* • *Has electromagnetic insulation been put in place?* • *Is the network components power supply properly controlled to ensure that it remains within the manufacturer's specifications?* • *Are the backup media protected from environmental damage?* • *Is the server facility kept free of dust, smoke and other matter, particularly food?*	*2*
Logical security control		
• *Passwords*	• *Are users assigned unique passwords?* • *Are users required to change the passwords on a periodic basis?* • *Are passwords encrypted and not displayed on the computer screen when entered?*	*2*
• *Network user access*	• *Is network user access based on written authorization and given on a need-to-know/need-to-do basis and based on the individual's responsibilities?*	*2*

	• *Are network workstations automatically disabled after a short period of inactivity?* • *Is remote access to the system supervisor prohibited?* • *Are all logon attempts to the supervisor account captured in the computer system?* • *Are activities by supervisor or administrative accounts subject to independent review?* • *Is up-to-date information regarding all communication lines connected to the outside maintained by the network supervisor?*	
• *Network access change requests*	• *Are network access change requests authorized by the appropriate manager? Are standard forms used?* • *Are requests for additions, changes and deletions of network logical access documented?*	*2*
• *Test plans*	• *Are appropriate implementation, conversion and acceptance test plans developed for the organization's distributed data processing network, hardware and communication links?*	*2*
• *Security reports*	• *Is only authorized access occurring?* • *Are security reports reviewed adequately and in a timely manner?* • *In the case of unauthorized users, are follow-up procedures adequate and timely?*	*2*
• *Security mechanisms*	• *Have all sensitive files/datasets in the network been identified and have the requirements for their security been determined?* • *Are all changes to the OS software used by the network and made by IS management (or at user sites) controlled? Can these changes be detected promptly by the network administrator or those responsible for the network?* • *Do individuals have access only to authorized applications, transaction processors and datasets?* • *Are system commands affecting more than one network site restricted to one terminal and to an authorized individual with an overall network control responsibility and security clearance?* • *Is encryption being used on the network to encode sensitive data?*	*2*

	• *Were procedures established to ensure effective controls over the hardware and software used by the departments served by the distributed processing network?* • *Are security policies and procedures appropriate to the environment:* *– Highly distributed?—Is security under the control of individual user management?* *– Distributed?—Is security under the direction of user management, but adheres to the guidelines established by IS management?* *– Mixed?—Is security under the direction of individual user management, but the overall responsibility remains with IS management?* *– Highly centralized?—Is security under the complete control of IS management?*	
• *Network operation procedures*	• *Do procedures exist to ensure that data compatibility is applied properly to all the network's datasets and that the requirements for their security have been determined?* • *Have adequate restart and recovery mechanisms been installed at every user location served by the distributed processing network?* • *Has the IS distributed network been designed to ensure that failure of service at any one site will have a minimal effect on the continued service to other sites served by the network?* • *Are there provisions to ensure consistency with the laws and regulations governing transmission of data?*	*2*
• *Interview the person responsible for maintaining network security*	• *Is the person aware of the risk associated with physical and logical access that must be minimized?* • *Is the person aware of the need to actively monitor logons and to account for employee changes?* • *Is the person knowledgeable in how to maintain and monitor access?*	*2*
• *Interview users*	• *Are the users aware of management policies regarding network security and confidentiality?*	*2*
[MAX Possible Mark Should NOT EXCEED 20]		

6. Protection of Information Assets **[20 Marks]**

An information security management system (ISMS) is a framework of policies, procedures, guidelines and associated resources to establish, implement, operate, monitor, review, maintain and improve information security for all types of organizations. An ISMS is defined in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series of standards and guidelines. Describes the related key elements of information security management.

Senior management leadership, commitment and support	*Commitment and support from senior management are important for successful establishment and continuance of an information security management program. This is commonly known as the "tone at the top."*	*[3]*
Policies and procedures	*The policy framework should be established with a concise top management declaration of direction, addressing the value of information assets, the need for security, and the importance of defining a hierarchy of classes of sensitive and critical assets. After approval by the governing body of the organization and by related roles and responsibilities, the information security program will be substantiated with the following:* • *Standards to develop minimum security baselines* • *Measurement criteria and methods* • *Specific guidelines, practices and procedures* *The policy should ensure resource conformity with laws and regulations. Security policies and procedures must be up to date and reflect business objectives, as well as generally accepted security standards and practices.*	*[3]*
Organization	*Responsibilities for the protection of individual assets should be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization and, where necessary, detailed guidance for specific sites, assets, services and related security processes, such as IT recovery and business continuity planning.*	*[3]*
Security awareness and education	*All employees of an organization and, where relevant, third-party users should receive appropriate training and regular updates to foster security awareness and compliance with written security policies and procedures. For new employees, this training should occur before access to information or service is granted. A number of different mechanisms available for raising security awareness include:*	*[3]*

	• *Regular updates to written security policies and procedures* • *Formal information security training* • *Internal certification program for relevant personnel* • *Statements signed by employees and contractors agreeing to follow the written security policy and procedures, including nondisclosure obligations* • *Use of appropriate publication media for distribution of security-related material (e.g., company newsletter, web page, videos, etc.)* • *Visible enforcement of security rules and periodic audits* • *Security drills and simulated security incidents*	
Risk management	*Processes should be in place to identify, assess, respond to and mitigate risk to information assets.*	*[2]*
Monitoring and compliance	*IS auditors are usually charged to assess, on a regular basis, the effectiveness of an organization's security program(s). To fulfill this task, they must have an understanding of the protection schemes, the security framework and the related issues, including compliance with applicable laws and regulations. As an example, these issues may relate to organizational due diligence for security and privacy of sensitive information, particularly as it relates to specific industries (e.g., banking and financial institutions, health care).*	*[3]*
Incident handling and response	*A computer security incident is an event adversely affecting the processing of computer usage. This includes loss of confidentiality of information, compromise of integrity of information, denial of service, unauthorized access to systems, misuse of systems or information, theft and damage to systems. Other incidents include virus attacks and intrusion by humans within or outside the organization*	*[3]*

End of Memorandum