NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty Computing and Informatics

DEPARTMENT OF INFORMATICS

QUALIFICATION: B.INFORMATICS HONOURS (WEB INFORMATICS); B. INFORMATICS HONS (BUS. INFORMATICS); POSTGRADUATE CERTIFICATE IN INFORMATICS (INFORMATION SYSTEMS AUDIT)	
QUALIFICATION CODE: 08BIFH/ 08BIHB/ 80BHBC/ 999NDP	**LEVEL:** 8
COURSE: Information Systems Audit	**COURSE CODE:** ISA822S
DATE: January 2019	**SESSION:** 2
DURATION: 3 Hours	**MARKS:** 75

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION PAPER	
EXAMINER(S)	Mr Pardon Blessings Maoneke
MODERATOR:	Mr Panduleni Ndilula

THIS QUESTION PAPER CONSISTS OF 7 PAGES
(Including this front page)

Instructions for the candidate

1. Answer **ALL** questions.
2. When writing take the following into account: The style should inform than impress, it should be formal, in third person, paragraphs set out according to ideas or issues and the paragraphs flowing in a logical order.
3. Information should be brief and accurate.
4. Please ensure that your writing is **legible**, **neat** and **presentable**.

SECTION A: Multiple Choice Questions. Each Question Carries One Mark [15 Marks]

1. To ensure disaster recovery is effective, it is **MOST** important that the business continuity plan and disaster recovery plan are:
   A. Stored at an alternate location
   B. Communicated to all users
   C. Tested regularly
   D. Updated regularly

2. During an IS audit, the IS auditor discovers that a wireless network is used within the enterprise's headquarters. What is the **FIRST** thing that the auditor should check for?
   A. The signal strength outside of the building
   B. The configuration settings
   C. The number of clients connected
   D. The IP address allocation mechanism

3. An IS auditor noticed that newly hired employees were sharing passwords while logging on to an application system, which is against company policy. What is the most effective control for this problem?
   A. Monitor access controls
   B. Providing security awareness training to users
   C. Assigning responsibility to the department head
   D. Training IT personnel

4. Which of the following is the **BEST** indicator of the effectiveness of backup and restore procedures while restoring data after a disaster?
   A. Members of the recovery team were available
   B. Recovery time objectives were met
   C. Inventory of backup tapes was properly maintained
   D. Backup tapes were completely restored at an alternative site

5. Which of the following **BEST** helps define disaster recovery strategies?
   A. Annual loss expectancy and exposure factor
   B. Maximum tolerable downtime and data loss
   C. Existing server and network redundancies
   D. Data backup and offsite storage requirements

6. Which of the following is the **MOST** effective preventive antivirus control?
    A. Scanning email attachments on the mail server
    B. Restoring systems from clean copies
    C. Disabling universal serial bus (USB) ports
    D. An online antivirus scan with up-to-date virus definitions

7. An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:
    A. Report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy
    B. Verify that user access rights have been granted on a need-to-have basis
    C. Recommend changes to the IS policy to ensure deactivation of user IDs upon termination
    D. Recommend that activity logs of terminated users be reviewed on a regular basis

8. An organization has outsourced its help desk activities. What is the IS auditor's **GREATEST** when reviewing the outsourcing contract and service level agreement?
    A. Documentation of staff background checks
    B. Independent audit report or full audit access
    C. Reporting the year-to-year incremental cost reductions
    D. Reporting staff turnover development or training

9. In planning an audit, the **MOST** critical step is the identification of the:
    A. Skill set of the audit staff
    B. Test steps in the audit
    C. Time allotted for the audit
    D. Areas of high risk

10. Which of the following outlines the overall authority to perform an IS audit?
    A. The audit scope, with goals and objectives
    B. A request from management to perform an audit
    C. The approved audit charter
    D. The approved audit schedule

11. Which of the following **BEST** provides access control to payroll data being processed on a local server
    A. Logging access to personal information
    B. Using separate passwords for sensitive transactions
    C. Using software that restricts access rules to authorized staff
    D. Restricting system access to business hours

12. An IS auditor suspects an incident (attack) is occurring while an audit is being performed on a financial system. What should the IS auditor do **FIRST**?
    A. Request that the system be shut down to preserve evidence
    B. Report the incident to management
    C. Ask for immediate suspension of the suspect account
    D. Immediately investigate the source and nature of the incident

13. For effective implementation after a business continuity plan (BCP) has been developed, it is **MOST** important that the BCP plan be:
    A. Stored in a secure, offsite facility
    B. Approved by senior management
    C. Communicated to appropriate personnel
    D. Made available through the enterprise's intranet

14. Which of the following represents an example of a preventive control with respect to IT personnel?
    A. Employing personnel that is qualified for its roles
    B. A log server which tracks logon IP addresses of users
    C. Review of visitor logs for the data center
    D. An accounting system which tracks employee telephone calls

15. Which of the following is a benefit of a risk-based approach to audit planning?
    A. Scheduling may be performed months in advance
    B. Resources are allocated to the areas of highest concern
    C. Budgets are more likely to be met by the IS audit staff
    D. Staff will be exposed to a variety of technologies

SECTION B: Scenario, Essay and Discussion **[60 Marks]**

QUESTION 1: Read the scenario 1 (one) below and answer the following questions. **[20 Marks]**

Ms Selma Shiponeni, the IT manager, is walking you (IS Auditor) through their SAP Enterprise Resource Planning change management. *Our SAP system works with three separate servers: the production server, development server and quality assurance server. SAP users who wish for any changes on the SAP system have to formally raise a request by logging in a fault at the help desk or simply fill out a job cut. The line manager has to approve the requested changes before the request is sent to the IT manager. The IT manager then authorizes one of the system designer and developer to make changes on the SAP system. These changes will be done on the SAP Development Server. Once changes are done, the IT manager will authorize the system designer and developer to transfer the SAP system from the SAP Development Server to the SAP Quality Assurance Server. The user who requested a change will be invited to test if the requested changes were effected accordingly. If the system user is happy, (s)he will sign of the job sheet acknowledging that the job was done properly. Once the system user has signed off the job, the following events will take place: the logged fault is closed, a summary of job done is filed, a new version of the SAP ERP is transferred from the quality assurance server to the production server.*

A. Identify and explain the evidence gathering technique used in scenario one. There is only one technique. **[3 Marks]**
B. Propose two possible control objective statements that befits the change management control in scenario one. **[4 Marks]**
C. Identify the category of the internal control used for the above system change management. **[2 Marks]**
D. Identify one example of objective evidence that could be used by an auditor from scenario one **[1 Mark]**
E. Explain the steps one can consider when doing a compliance test on the above scenario. **[10 Marks]**

QUESTION 2 **[20 Marks]**

A. Propose one or more actions and recommendations that could be considered by an auditor under the following scenarios during an audit excise:

I. An IS auditor found that audit tests on a web-based order system shortly before the scheduled go-live date produces inconclusive results and additional testing cannot be concluded by the completion date agreed for the audit. **[2 Marks]**

II. An IS auditor identifies a major control deficiency in the change management software that supports the accounting application. **[2 Marks]**

III. An IS auditor discovers that devices connected to the network have not been included in a network diagram that had been used to develop the scope of the audit. The Chief Information Officer explains that the diagram is being updated and awaiting final approval. **[3 Marks]**

IV. Corporate IS policy for a call center requires that all users be assigned unique user accounts. On discovering that this is not the case for all current users, which is the **MOST** appropriate recommendation? **[2 Marks]**

B. Discuss the organization of an IS audit function clearly indicating its main components. **[5 Marks]**

C. State and explain any three categories of incidents that may not be part of an IT Business Continuity Plan. **[6 Marks]**

QUESTION 3 **[20 Marks]**

A. State and explain any **FOUR** performance IS auditing standards that you are aware of **[8 Marks]**

B. Under what circumstances should one consider substantive testing over compliance testing? **[2 Marks]**

C. State and explain any **FIVE** evidence gathering techniques you know **[10 Marks]**

The End of The Exam