NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF INFORMATICS

QUALIFICATION : POST GRADUATE CERTIFICATE IN INFORMATICS (INFORMATION SYSTEMS AUDIT)	
QUALIFICATION CODE: 08PGCI	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE NAME:** INFORMATION SYSTEMS AUDIT
SESSION: JUNE 2019	**PAPER:** THEORY
DURATION: 3 HOURS	**MARKS:** 100

FIRST OPPORTUNITY 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. Answers should be neat, relevant and brief 5. In marking, the Examiners will take into account clarity of exposition, logic of arguments, effective presentation and language use.

PERMISSIBLE MATERIALS

None

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

SECTION A: MULTIPLE CHOICE **[20]**

Question 1: Multiple choice **[20]**

1. Which of these choices is the *best* answer regarding who is primarily responsible for providing internal controls to detect, correct, and prevent irregularities or illegal acts?
   A. Board of directors
   B. Information technology
   C. Legal, also known as general council
   D. Human resources

2. Which of the following functions should be separated from the others if segregation of duties cannot be achieved in an automated system?
   A. Origination
   B. Authorization
   C. Reprocessing
   D. Transaction logging

3. What is the purpose of the audit committee?
   A. To provide daily coordination of all audit activities
   B. To challenge and review assurances
   C. To assist the managers with training in auditing skills
   D. To govern, control, and manage the organization

4. How should management act to best deal with emergency changes?
   A. Emergency changes cannot be made without advance testing.
   B. The change control process does not apply to emergency conditions.
   C. All changes should still undergo review.
   D. Emergency changes are not allowed.

5. What is the best definition of auditing?
   A. Review of past history using evidence to tell the story.
   B. Forecasting compliance generated by a new system preparing to enter production.
   C. Pre-compliance assessment based on management's intended design.
   D. Certification testing of the system benefits or failures.

6. What are three of the four key perspectives on the IT balanced scorecard?
   A. Business justification, service-level agreements, budget.
   B. Organizational staffing, cost reduction, employee training.
   C. Cost reduction, business process, growth.
   D. Service level, critical success factors, vendor selection.

7. Which sampling method is used when the likelihood of finding evidence is low?
   A. Discovery
   B. Cell
   C. Random
   D. Stop and go

8. When auditing the use of encryption, which of the following would be the primary concern of the auditor?
   A. Management's level of control over the use of encryption
   B. Strength of encryption algorithm in use
   C. Key sizes used in the encryption and decryption process
   D. Using the correct encryption method for compliance

9. Which of the following represents the hierarchy of controls from highest level to lowest level?
   A. General, pervasive, detailed, application
   B. Pervasive, general, application, detailed
   C. Detailed, pervasive, application, detailed
   D. Application, general, detailed, pervasive

10. What is the primary objective in the third phase of incident response?
   A. Containment
   B. Lessons learned
   C. Eradication
   D. Analysis

11. What is the first priority of management upon the possible detection of an irregular or illegal act?
   A. Shut down access to the system.
   B. Aid the process of investigation and inquiry.
   C. Notify appropriate law enforcement.
   D. Contact auditors to schedule an audit of the situation.

12. Which of the following is not one of the three major control types?
   A. Detective
   B. Deterrent
   C. Preventive
   D. Corrective

13. Which method of backup should be used on a computer hard disk or flash media prior to starting a forensic investigation?
    A. Full
    B. Differential
    C. Bitstream
    D. Logical

14. In regard to the IT governance control objectives, which of the following occurrences would the auditor be most concerned about during execution of the audit?
    A. Using the practice of self-monitoring to report problems
    B. Using proper change control
    C. Conflict in the existing reporting relationship
    D. Production system without accreditation

15. 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

16. In performing a risk-based audit, which risk assessment is completed initially by the IS Auditor?
    A. Detection risk assessment
    B. Control risk assessment
    C. Inherent risk assessment
    D. Fraud risk assessment

17. The approach an IS auditor should use to plan IS audit coverage should be based on:
    A. risk.
    B. materiality.
    C. professional scepticism.
    D. sufficiency of audit evidence

18. A company performs a daily backup of critical data and software files and stores the backup tapes at an offsite location. The backup tapes are used to restore the files in ease of a disruption. This is a:
    A. preventive control.
    B. management control,
    C. corrective control.
    D. detective control.

19. The MOST important responsibility of a data security officer in an organization is:
    A. recommending and monitoring data security policies.
    B. promoting security awareness within the organization.
    C. establishing procedures for IT security policies.
    D. administering physical and logical access controls.

20. What is considered the MOST critical element for the successful implementation of an information security (IS) program?
    A. An effective enterprise risk management (ERM) framework
    B. Senior management commitment
    C. An adequate budgeting process
    D. Meticulous program planning

SECTION B: SHORT STRUCTURED QUESTIONS **[30]**

Question 2 **[30]**

a) Testing all aspects of the DRP is the most important factor in achieving success in an emergency situation. Explain 5 types of disaster recovery tests (10)

b) How should the evidence gathered during the audit be kept safe? (03)

c) Organization policies, standards and procedure play a role in auditing of governance enterprise, what are the areas auditor look at when auditing policies? (07)

d) What is the difference between incident management and problem management? (04)

e) What is job scheduling? What are the four advantages of using job scheduling software? (06)

SECTION C: LONG STRUCTURED QUESTIONS **[50]**

Question 3 **[10]**

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. Briefly outline five potential tasks that an auditor may undertake during system development, acquisition and maintenance.

Question 4 **[10]**

An IS auditor was asked to review alignment between IT and business goals for a small financial institution. The IS auditor requested various information including business goals and objectives and IT goals and objectives. The IS auditor found that business goals and objectives were limited to a short-bulleted list, while IT goals and objectives were limited to slides used in meetings with the CIO (the CIO reports to the CFO). It was also found in the documentation provided that over

the past two years, the risk management committee (composed of senior management) only met on three occasions, and no minutes of what was discussed were kept for these meetings. When the IT budget for the upcoming year was compared to the strategic plans for IT, it was noted that several of the initiatives mentioned in the plans for the upcoming year were not included in the budget for that year.

a) Explain which concern should be of GREATEST concern to the IS auditor? (5)
b) Explain which issue would be the MOST significant issue to address? (5)

Question 5 **[10]**

A major financial institution has just implemented a centralized banking solution (CBS) in one of its branches. It has a secondary concern to look after marketing of the bank. Employees of a separate legal entity work on the bank premises, but they have no access to the bank's solution software. Employees of other branches get training on this solution from this branch and for training purposes temporary access credentials are also given to such employees. IS auditors observed that employees of the separate legal entity also access the CBS software through the branch employees access credentials. IS auditors also observed that there are numerous active IDs of employees who got training from the branch and have since been transferred to their original branch.

a) As an IS Auditor, explain the negative impact of password sharing and explain what you would recommend to the bank to effectively eliminate the practice of password sharing?(5)
b) How BEST would you address the issue of user ID management of trainee employees? (5)

Question 6 **[20]**

Information security has now become a significant governance issue as a result of global network, rapid technological innovation and change, increased dependence on IT, increased sophistication of threat agents, and an extension of the enterprise beyond its traditional boundaries. Due to importance of information security, banking management has created a post of Chief Information Officer (CIO) and Mr. Yaseen is appointed for this post. CIO just after his appointment established a steering committee.

Discuss in detail the role and responsibilities, authority and membership of ' IT steering committee' in the banking organization.

End of question paper