NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF INFORMATICS

QUALIFICATION: Postgraduate Certificate in Informatics (Information Systems Audit)	
QUALIFICATION CODE: 08PGIN	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE NAME:** Information Systems Audit
SESSION: JULY 2024	**PAPER:** PAPER 1
DURATION: 3 HOURS	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mrs Ruusa Ipinge**
MODERATOR:	**Mr Panduleni Ndilula**

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

THIS QUESTION PAPER CONSISTS OF 9 PAGES (Including this front page)

PART 1: MULTIPLE QUESTIONS (40 MARKS MAXIMUM, 2 MARKS FOR EACH CORRECT ANSWER). Answer all questions. Select ONLY ONE BEST ANSWER to each question.

1. **The procedures performed by an auditor when testing a control should be documented in a**:
   b) Working paper
   c) Audit charter
   d) Management letter
   e) None of the above

2. **Reviewng a specific policy to understand the scope of the policies in place.**
   a) A policy audit,
   b) Policy review,
   c) Procedures,
   d) Guideline.

3. **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, aka general council
   d) Human resources

4. **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

5. **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

6. **Which of the following is not one of the three major control types?**

a) Detective

b) Deterrent

c) Preventive

d) Corrective

7. **Which of the following options is *not* true regarding configuring routers, servers? workstations, printers, and networked databases set up using default settings.**

a) Designed to reduce technical support during installation for novice users.

b) Sufficient controls to provide a minimum level of safety for production use.

c) Predictable to facilitate successful intrusion attacks using well-known filenames, access paths, and missing or incomplete security parameters.

d) Remote scanning and automated penetration tools that prey upon systems running on default settings.

8. **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 under any condition.

9. **Which of the following would be a concern that the auditor should explain in the audit report along with their findings?**

a) Lack of a detailed list of audit objectives

b) Undue restrictions placed by management on evidence use or audit procedure.

c) Communicating results directly to the chairperson of the audit committee

d) Need by the current auditor to communicate with the prior auditors.

10. During the performance of an audit, a reportable finding is identified with the auditee. The auditee immediately fixed the problem upon identification. Which of the following is true because of this interaction?

a) Auditee resolved the problem before the audit report is written, therefore no finding exists.

b) Auditor can verify that the corrective action has been taken before the audit report is written, therefore no finding exists.

c) Auditor includes the finding in the final audit report as resolved.

d) Auditor lists the finding as it existed.

11. Which of the following management methods provides the most control rather than discretionary flexibility?

a) Distributed

b) Centralized

c) In-house

d) Outsourced

12. What is the principal issue surrounding the use of CAAT software?

a) The capability of the software vendor

b) Documentary evidence is more effective.

c) Inability of automated tools to consider the human characteristics of the environment

d) The possible cost, complexity, and security of output

13. Digital signatures are designed to provide additional protection for electronic messages inorder to determine which of the following?

a) Message read by unauthorized party

b) Message sender verification

c) Message deletion

d) Message modification

14. Which is the primary benefit of using a risk-based approach in audit planning?

a) Simplifies resource scheduling.

b) Allocates resources to the areas of highest concern.

c) Properly trained personnel are available.

d) Lowers the overall cost of compliance.

15. What indicators are used to identify the anticipated level of recovery and loss at a given point in time?

a) RPO and RTO

b) RTO and SDO

c) RPO and ITO

d) SDO and IRO

16. Which of the following is the best choice to ensure that internal control objectives are met?

a) Top executive issues a policy stating compliance objectives.

b) Procedures are created to govern employee conduct.

c) Suitable systems for tracking and reporting incidents are used.

d) The clients operating records are audited annually.

17. Which of the following statements is true concerning asymmetric key cryptography?

a) The sender encrypts the files by using the recipient's private key.

b) The sender and receiver use the same key.

c) Asymmetric keys cannot be used for digital signatures.

d) The sender and receiver have different keys.

18. Who is responsible for designating the appropriate information classification level?

a) Data custodian

b) Data user

c) Data owner

d) Security manager

19. Where should the computer room be located?

a) Secure basement

b) First floor

c) Middle floor

d) Top floor

20. What is the purpose of performing a post-implementation review?

a) To gather requirements.

b) To assess whether objectives have been met.

c) To identify future iterations.

d) None of the above.

PART 2: WRITTEN OR ESSAY QUESTIONS (35 MARKS ALLOCATED)

ANSWER ALL QUESTIONS

1. Explain what Pre-Audit Planning means and list two of its activities. [3]
2. Explain the following term [4]
   a) Audit Program
   b) Automated Control
   c) Audit Charter
   d) Fieldwork
3. ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations worldwide, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programme modules, and draft agreements are all preserved and administered in the e-form only. The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

   a) Explain the first 5 phases of System Development Life Cycle (SDLC), that Ask International could use to develop its software [10]

   b) Suppose an audit policy is required, how will you lay down the responsibility of audit? [5]
4. Explain the roles of the information System Audit [7]
5. Using examples explain the difference between internal Audit and External Audit [6]

PART 3: GENERAL AND CASE STUDY BASED QUESTIONS (25 MARKS ALLOCATED)

Case Study: Target Corporation Data Breach

In 2013, Target Corporation suffered a massive data breach that compromised the personal and financial information of 40 million customers. The attack was carried out by cybercriminals who gained access to Target's payment system through a third-party vendor. The incident resulted in significant financial losses for the company, as well as damage to its reputation and customer trust.

One of the key factors contributing to the Target data breach was a failure of IT governance. Despite having various policies and procedures in place to protect customer data, the company had failed to implement effective controls to monitor and enforce compliance with these policies. Target had failed to properly segregate its payment system from the rest of its network, which allowed the attackers to gain access to sensitive data. In addition, the company had failed to implement two-factor authentication for accessing its payment system, which would have made it more difficult for the attackers to gain access.

The incident highlighted the importance of IT governance in preventing data breaches. Target subsequently implemented a number of changes to improve its IT governance, including:

1.The appointment of a Chief Information Security Officer (CISO) to oversee the company's cybersecurity strategy and ensure compliance with relevant regulations and standards.

2.The implementation of two-factor authentication for accessing the payment system, which helps to prevent unauthorized access to sensitive data.

3.The implementation of a more robust intrusion detection system, which allows the company to detect and respond to security incidents more quickly.

The implementation of a more comprehensive training and awareness program for employees, which helps to ensure that everyone understands their responsibilities when it comes to data security

The incident highlighted the importance of IT governance in preventing data breaches. Target subsequently implemented a number of changes to improve its IT governance. Through these measures, Target was able to improve its IT governance and prevent future data breaches. The incident served as a wake-up call for other organizations, highlighting the importance of IT governance and the potential consequences of failure to properly manage information and technology assets.

Read the case study above and answer the questions below. Note that some questions require your general knowledge.

1. Explain the components that comprise IT Governance according to the target corporation. [2]
2. Explain the three factors of the target corporation that contributed to the failure of the Data Breach [3]
3. Give **four** areas that could be part of the database audit [4]
4. Explain the critical components of the business continuity plan. [8]
5. A business continuity plan will be required to restore all possible data lost. You are appointed to audit the business continuity plan. Explain how you would audit a business continuity plan. [8]

END OF QUESTION PAPER