NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF INFORMATICS

QUALIFICATIONS: Postgraduate Certificate in Informatics (Information Systems Audit)	
QUALIFICATION CODE: 08PGIN	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE:** Information Systems Audit
DATE: June 2023	**SESSION:** 1
DURATION: 3 Hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINERS:	Mrs Ruusa Ipinge
MODERATOR(S):	Mr Panduleni Ndilula

THIS EXAMINATION PAPER CONSISTS OF 9 PAGES
(INCLUDING THIS FRONT PAGE)

INSTRUCTIONS FOR THE CANDIDATE

1. Answer ALL QUESTIONS.
2. When writing, take 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**.

PART 1: MULTIPLE QUESTIONS (40 MARKS MAXIMUM 2 MARK FOR EACH CORRECT ANSWER)

Answer all questions. Select ONLY ONE BEST ANSWER to each questions.

1. **An IS auditor is reviewing the physical security controls of a data centre and notices several areas for concern. Which of the following areas is the MOST important?**

   a. The emergency power off button cover is missing.

   b. Scheduled maintenance of the fire suppression system was not performed.

   c. There are no security cameras inside the data centre.

   d. The emergency exit door is blocked.

2. **IT audit is the process of collecting and evaluating evidence to determine**

   a) Whether a computer system safeguards assets

   b) Whether maintains data integrity

   c) Whether allows organizational goals to be achieved effectively and uses resources efficiently

   d) All of the above

3. **The FIRST priority of the IS auditor in year one should be to study the:**

   A. previous IS audit reports and plan the audit schedule.

   B. audit charter and plan the audit schedule.

   C. impact of the increased employee turnover.

   D. impact of the implementation of a new ERP on the IT environment.

4. **Which of the following BEST describes an IT department's strategic planning process?**

a) The IT department will have either short- or long-range plans depending on the organization's broader plans and objectives.

b) The IT department's strategic plan must be time- and project oriented but not so detailed as to address and help determine priorities to meet business needs.

c) Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements.

d) Short-range planning for the IT department does not need to be integrated into the short-range plans of the organization since technological advances will drive the IT department plans much quicker than organizational plans.

5. **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.

6. **Which of the following is the MOST critical control over database administration (DBA)?**

a) Approval of DBA activities

b) Segregation of duties in regard to access rights granting/revoking

c) Review of access logs and activities

d) Review of the use of database tools

7. **Risk-Control-Matrix is developed in which step of IS audit**

a. Analysis

b. Planning

c. Fieldwork

d. Reporting

8. **Which one is not the objective of Audit Trail?**

a) Audit trail promotes Personal Accountability

b) Audit detects Unauthorized Access

c) To promote good internal control

d) Audit trail facilitates the reconstruction of events

9. **Which of the following is the PRIMARY purpose for conducting parallel testing?**

a) To determine whether the system is cost-effective

b) To enable comprehensive unit and system testing

c) To highlight errors in the program interfaces with files

d) To ensure the new system meets user requirements

10. **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 case of a disruption. This is a:**

a. Preventive control.

b. Management control.

c. Corrective control.

d. Detective control.

11. **The FIRST step in planning an audit is to:**

a. Define finding.

b. Finalize the audit scope and audit objectives.

c. Gain an understanding of the business' objectives.

d. Develop the audit approach or audit strategy.

12. **The objectives of an IT audit include**

a. Ensures asset safeguarding

b. Ensures that the attributes of data or information are maintained

c. Both (a) and (b)

d. None of the above

13. **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.

14. **The IS scope should outline the:**

a. The findings identified by the Auditor.

b. The systems in scope, controls to be tested, timelines and objective of the audit.

c. The authority of the IS audit function.

d. The IS auditor's CV.

15. **Why should a BCP be tested?**

a) To identify a future incident.

b) To train employees.

c) To identify limitations and improvement areas.

d) To assess the competence of the CEO.

16. **Which of the following can increase capacity and reliability of an application?**

a) Live replication to various geographic regions.

b) Load balancing.

c) Clustering.

d) None of the above

17. **Raised floors, fire suppression systems, and air cooling systems are examples?**

a) Access control.

b) Change management.

c) Environmental controls.

d) Voice over IP (VoIP).

18. Requiring a password, and code sent to your phone in order to use an application is an example of?

a) Multifactor authentication.

b) Single sign-on.

c) Two-factor authentication.

d) Native authentication.

19. Which of the following is an example of social engineering?

a) Penetration testing

b) Tailgating

c) VPN

d) Logging

20. Which of the following weaknesses would be considered the MOST serious in enterprise resource planning (ERP) software used by a bank?

a) Access controls have not been reviewed.

b) Limited documentation is available.

c) Two-year-old backup tapes have not been replaced.

d) Database backups are performed once a day.

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

ANSWER ALL QUESTIONS

1. Using really example explain the following term   [8]

    a)   Audit Charter;

    b)   Automated Controls

    c)   Working paper;

    d)   Audit plan

2. The IS auditor advised the CIO and team to improve the general IT control environment. COBIT was proposed to be adapted. What recommendations would the IS auditor make when considering this framework?   [4]

3. The audit plan provides the procedures that need to be followed to complete the work. The purpose of a plan is to outline clear roles and responsibilities. List and explain the 5 planning areas that are likely to be discussed during the audit process   [10]

4. Differentiate between Deviation and Deficiency in a a context of design of a control   [4]

5. An internal control system should be designed to meet a firm's specific informational needs. Using example, list and explain the types of internal controls   [9]

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

Goldoson MalwareStore

Security researchers have discovered a new malicious software library capable of collecting lists of installed applications, a history of Wi-Fi and Bluetooth device information as well as nearby GPS location data. Dubbed Goldoson by McAfee's Mobile Research Team confirmed that the library can also load web pages without user awareness and perform advertisement fraud by clicking on ad links in the background without the victim's consent.

"The research team has found more than 60 applications containing this third-party malicious library, with more than 100 million downloads confirmed in the ONE store and Google Play app download markets in South Korea," wrote McAfee's SangRyol Ryu. "While the malicious library was made by someone else, not the app developers, the risk to installers of the apps remains. "From a technical standpoint, the Goldoson library registers the device and gets remote configurations while the app runs. "The library name and the remote server domain vary with each application and are obfuscated. The name Goldoson is after the first found domain name," Ryu explained.

Further, remote configuration contains the parameters for each functionality, specifying how often it runs the components. "Based on the parameters, the library periodically checks, pulls device information, and sends them to the remote servers," reads the advisory. For instance, collected data is sent out every two days by default, but the cycle can be changed by the remote configuration. The McAfee team said it notified Google of the malicious apps. As a result of the disclosure, some apps were removed from Google Play while others were updated by the official developers.

"As applications continue to scale in size and leverage additional external libraries, it is important to understand their behavior," Ryu concluded. "App developers should be upfront about libraries used and take precautions to protect users' information." The Goldoson library disclosure comes a couple of months after Kaspersky security researchers announced the discovery of 196,476 new mobile banking Trojan installers in 2022, doubling the number observed in 2021.

Read the case study above and answer the questions below, note some questions requires your general knowledge

1. What is a Malicious Software [1]

2. Demonstrate how the malware attacked the google play app? [2]

3. Social engineering exercises have resulted in corporations losing millions of dollars in revenue. Explain 4 examples of social engineering, specifically the one that might have led to the attack in the above case studies [8]

4. Explain the benefits of Good IT governance [4]

5. Using a real example, what are the 6 cloud storage security risks? [6]

6. Why should the Play Store App carry out Business Impacts Analysis (BIA) [4]

END OF QUESTION PAPER