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: JUNE 2024	**PAPER:** PAPER 1
DURATION: 3 HOURS	**MARKS:** 100

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

INSTRUCTIONS
1. Answer ALL the questions. 2. Read all the questions carefully before answering. 3. Number the answers clearly

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. **An audit project has been taking far too long, and management is beginning to ask questions about its schedule and completion. This audit may be lacking:**
   a) Effective project management
   b) Cooperation from individual auditees
   c) Enough skilled auditors
   d) Clearly stated scope and objectives

1.

2. **During an IS risk assessment of a health care organisation regarding protected health care information (PHI), an IS auditor interviews IS management. Which of the following findings from the interviews would be of MOST concern to the IS auditor?**

   a. The organization does not encrypt all of its outgoing email messages.

   b. Staff must type "[PHI]" in the subject field of email messages to be encrypted.

   c. An individual's computer screen saver function is disabled.

   d. Server configuration requires the user to change the password annually.

3. **Which of the following is the responsibility of information asset owners?**

   a. Implementation of information security within applications

   b. Assignment of criticality levels to data

   c. Implementation of access rules to data and programs

   d. Provision of physical and logical security for data

4. **With the help of a security officer, granting access to data is the responsibility of**

   a. Data owners

   b. Programmers

   c. Systems analysts

   d. Librarians

5. **The FIRST step in data classification is to**

a. Establish ownership.

b. Perform a criticality analysis.

c. Define access rules.

d. Create a data dictionary.

6. **Which of the following would MOST effectively reduce social engineering incidents?**

a. Security awareness training

b. Increased physical security measures.

c. Email monitoring policy

d. Intrusion detection system

7. **Which of the following acts as a decoy to detect active Internet attacks?**

a. Honeypots

b. Firewalls

c. Trapdoors

d. Traffic analysis

8. **Which of the following is the BEST way for an IS auditor to determine the effectiveness of a security awareness and training program?**

a. Review the security training program.

b. Ask the security administrator.

c. Interview a sample of employees

d. Review the security reminders to employees.

9. **As his company's Chief Information Security Officer (CISO), George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?**

a. threats x vulnerability X asset value = residual risk

b. SLE x frequency = ALE, which is equal to residual risk

c. (threats x vulnerability x asset value) x control gap = residual risk

d. (total risk – asset value) x countermeasures = residual risk

10. **An IS auditor is reviewing the physical security controls of a data center 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 center.
d. The emergency exit door is blocked.

11. **Involves reviewing a specific policy to understand the scope of the policies in place.**

a) A policy audit,
b) Policy review,
c) Procedures,
d) Guideline

12. **Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files. Choos the BEST.**

a) Confidentiality
b) Integrity
c) Redundancy
d) Concurrency

13. 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.

14. The following are threats to Information Security except:

a) Virus Attacks

b) Lack of adequate resources.

c) Natural Disasters

d) Theft, Sabotage and Misuse

15. 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

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

a. Analysis

b. Planning

c. Fieldwork

d. Reporting

17. The responsibility of information security lies within the

a) Chief Information Officer

b) Chief Executive Officer

c) Managers

d) All employees

18. 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).

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

a) Multifactor authentication.
b) Single sign-on.
c) Two-factor authentication.
d) Native authentication.

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

a) Penetration testing
b) Tailgating
c) VPN
d) Logging

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

ANSWER ALL QUESTIONS

1. Explain the following term [7]
   a. Audit Charter. (2)
   b. Automated Controls (2)
   c. Work paper. (2)
   d. Business case (1)

2. Authentication is the bedrock or first to access a corporate network or information system. Explain the two types of authentication enforced by information system security. [4]

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

4. Using an example, differentiate between Compliance and Forensic audit. [6]

5. Using examples, differentiate between statistical and none statistics sampling: [8]

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

Another day, another security scare for Android users. Hot on the heels of yesterday's Pokemon Go malicious app news, researchers have uncovered more rogue apps in the Google Play Store.

Researchers from Lookout's Security Research & Response team identified a piece of spyware hiding in four apps available in Google's official app store. The spyware has been dubbed Overseer and is capable of stealing "significant amounts" of personal data from users.

This data includes: The user's contacts, including name, phone number, email, and times contacted; all user accounts on a compromised device; precise location, including latitude, longitude, network ID, and location area code; free internal and external memory; Device IMEI, IMSI, MCC, MNC, phone type, network operator, device and Android information; and details of installed packages, Lookout researchers outlined in a blog.

Lookout says the spyware specifically targets foreign travellers; one app it was found hiding in was designed to help travellers find their country's embassy when abroad. Overseer was also found in Russian and European news apps.

What's worth pointing out about this malware is how it communicated with its command-and-control centre. In this case, the C&C was running on Facebook's Parse Server, which is hosted on Amazon Web Services. This means that the traffic between the spyware and the C&C looks legitimate, and would be less likely to be stopped.

Lookout didn't release any details of how many downloads the apps had, or how many devices were potentially affected. Google has removed the apps from the Google Play Store.

This is the latest in a long list of malicious apps to target Android users. Most recently, Kaspersky researchers found a rogue app disguised as a Pokemon Go guide. That app was capable of installing and uninstalling apps and displaying adverts.

Unofficial Android app stores have long been criticized for the number of malicious apps that appear in them, and Android malware is rapidly becoming a big problem for users and businesses alike. It is advisable to only download applications from the official Google Play Store, although as this shows, that too is not safe from malware.

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

1. What is a spyware? [1]
2. Demonstrate how the malware attacked Android users. [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. Using examples, Explain the 2 audit standards according to ISACA. [4]
5. Explain three of the rights of Data Subjects according to the General Data Protection Regulation. [6]
6. How could an organisations prevent the malicious software [4]

END OF QUESTION PAPER