



**NAMI BIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY**

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF INFORMATICS, JOURNALISM AND MEDIA TECHNOLOGY

QUALIFICATION : POST GRADUATE CERTIFICATE IN INFORMATICS (INFORMATION SYSTEMS AUDIT)	
QUALIFICATION CODE: 08PGIN	LEVEL: 8
COURSE: INFORMATION SYSTEMS AUDITING	COURSE CODE: ISA822S
DATE: JULY 2022	SESSION: 1
DURATION: 3 HOURS	MARKS: 100

SECOND OPPORTUNITY/SUPPLEMENTARY QUESTION PAPER	
EXAMINER(S)	MRS RUUSA IPINGE
MODERATOR:	MR PANDULENI NDILULA

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

INSTRUCTIONS

- Answer ALL questions in Part 1, Part 2 and Part 3,
- MUST examinations rules apply
- DO NOT open this examination cover until you are instructed to do so.
- DO NOT FORGET to write down your student number at the designated places in the examination page.

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 should ensure that IT governance performance measures:**
 - A. evaluate the activities of IT oversight committees.
 - B. provide strategic IT drivers.
 - C. adhere to regulatory reporting standards and definitions.
 - D. evaluate the IT department.

2. **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

3. **An IS auditor is assigned to audit a software development project, which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?**
 - a) Report that the organization does not have effective project management.
 - b) Recommend the project manager be changed.
 - c) Review the IT governance structure.
 - d) Review the conduct of the project and the business case

4. **Which of the following choices BEST helps information owners to properly classify data?**
 - a) Understanding of technical controls that protect data
 - b) Training on organizational policies and standards
 - c) Use of an automated data leak prevention (DLP) tool
 - d) Understanding which people need to access the data

- 5. What is the process of extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions?**
- a) Big Data
 - b) Business intelligence
 - c) Electronic Data interchange
 - d) Machine Learning
- 6. 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.
- 7. The FIRST step in planning an audit is to:**
- a) define audit deliverables.
 - b) finalize the audit scope and audit objectives.
 - c) gain an understanding of the business' objectives.
 - d) develop the audit approach or audit strategy.
- 8. 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.

9. 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

10. What is the first step in performing a risk assessment?

- a) Risk treatment
- b) Risk evaluation
- c) Risk response
- d) Risk identification

11. 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.

12. Which of the following can increase capacity and reliability of an application? Choose the best answer.

- a) Live replication to various geographic regions.
- b) Load balancing.
- c) Clustering.
- d) None of the above.

13. 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).

14. 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.

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

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

16. The following is an example of a cloud service model

- a) DEFI.
- b) Private cloud.
- c) Infrastructure as a Service.
- d) None of the above.

17. The waterfall software development model is appropriate when:

- a) Requirements are well defined and do not change.
- b) Requirements are constantly changing.
- c) Unit tests are performed in iterations.
- d) Prototypes are not required.

18. A challenge commonly associated with the Agile development model is

- a) Lack of communication.
- b) Lack of documentation.
- c) Lack of testing.
- d) Lack of resources.

19. Who should approve the implementation of a system?

- a) The receptionist.
- b) The CEO.
- c) Board members.
- d) Project Manager.

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 [8]
 - a) Standard.
 - b) Working paper.
 - c) Audit Charter.
 - d) Fieldwork.
3. Edgars faces a lack of data, insufficient historical records, and/or unreliable data. A lack of data has contributed to poor performance, sales, and poor decision making. This issue can be effectively addressed through the use of data collection tools. The risk has been assessed against company policies and it has been found that risk transfer is required, i.e., a third party needs to be engaged to collect the data.
- 3.1 There are three stages or phases in conducting a risk assessment. Using the scenario described above, identify and describe these stages and provide an example of each stage as described in the case study [9]
4. By use of example list and explain the three Categories of Audit Controls [9]
5. Using examples explain the difference between Compliance and Forensics Audit [6]

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

Data Backup and Restoration Strategy

When it comes to the banking sector having a data backup and restoration strategy is important. A data administrator has the responsibility to prepare for the possibility of hardware, software or media failure as well as the recovery databases during a disaster. Here, the data backup and restoration strategy is discussed under four main criteria.

First decide what needs to be backed-up. The database administrator should have a clear idea about which databases, related operating systems and application components have to be backed up. There should be an online backup as well as an offline backup. In MySQL server databases need to backup both system and user databases. With that, there should be a separate maintenance plan for system databases. In addition, there should be a backup of all user databases, including database and transactions logs that records all database modifications and a recovery model set, (Navid Akhtar et al., 2012).

Two types of backup can be applied, these are logical backup and physical backup in MySQL servers. In the logical backup, the flat files can be restored using Export and Import Wizard, SQL Server Integration Services Tools. In the physical backup both databases and transactions logs can be backed up and restored to the database in the point of failure. And this can be used for very large databases, (Navid Akhtar et al., 2012). Establishing a strategy for handling exceptionally large database backups is essential when implementing a database backup and restoration strategy in a bank. With regards to MySQL the database can be partitioned for multiple files and then backed-up, (Navid Akhtar et al., 2012). The weekly backup cycle can be implemented for a full backup on Friday night or Saturday morning and differentiate backups on weekdays, (Navid Akhtar et al., 2012).

Though it is not popular in Sri Lanka, the best place to store backups is the cloud. With the limited bandwidth and internet speed we have it is hard to have that kind of storing process in the cloud. But as another option, we are having a practice to backup to a disk, transfer to a tape and store tapes offsite for disaster recovery processes. (Navid Akhtar et al., 2012). And then it is required to develop a backup retention policy. Based on the criteria which have to be chosen carefully, to make sure that, these are compliant with the backup media subsystem retention policy and

requirements for the backup recovery strategy, (Navid Akhtar et al., 2012). Through scheduling maintenance plans for backups in MySQL servers, the backup process can be effectively maintained through automation process. Further, monitoring backups, reviewing backup logs and catalogues are also supported to increase the efficiency of backup process.

A restoration testing technique should be implemented. So, there must be a requirement to test database restoration from disk as well as from tape backups. (Navid Akhtar et al., 2012). This can be identified as a key element of whole data recovery process. So companywide stakeholders are well informed about the disaster recovery plan, (Navid Akhtar et al., 2012). This ongoing, active and collaborative effort between the internal audit and database administration team of the company can guarantee the security, management and recovery data in the event of a disaster.

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

1. What is a transactional log? [2]
2. What are the three factors that you need to consider when choosing the type of a backup, that can be performed by your company? [3]
3. According to Navid, how can a backup be maintained? [3]
4. Give three areas that could be part of the database audit. [4]
5. Give the three types of backup procedures. [3]
6. ISO 22300 defines the Recovery Time Objective (RTO) as the period of time following an incident within which a product and service or an activity is resumed or resources are recovered 2021. List and Explain **five** of RTOs strategy that the organisation should utilise. [10]

END OF QUESTION PAPER