Advanced Information Systems Audit
Final examination
2 Hours 30 Minutes

A. This examination consists of questions on material taught through the lecture sessions and associated references.
   - **Part A** (30 Marks) is composed of multiple choice questions;
   - **Part B** (70 Marks) requires detailed, complete and correct answers. Be concise with your answers by using the fewest words possible to provide the detailed, complete and correct answers.

B. You are required provide detailed, complete and correct answers to the questions

C. You must work individually. The order of questions neither corresponds with the order of the course material nor associated difficulty.

D. This is a closed book examination and no reference materials are allows in the examination room. No books, no course notes or printouts of any kind. No calculators, no cellphones/smartphones, computers, or electronic devices of any kind. You must turn off any electronic devices and store them under your desk simply having any device (even if turned off) with you during the exam constitutes a violation and will be reported. If you need to borrow a pencil, sharpener, eraser, etc., you must ask a proctor. You are not allowed to directly talk to any of your neighbours in the examination room.

E. Before, during, and at the end of the examination:
   - You are not allowed to leave the examination room during the examination room period, except for visits to the washrooms.
   - Please do not stand up or talk until all examinations are is picked up; this also applies to cases where you finish earlier than the allotted period.
   - Ask the proctor questions that are meaningful in the context of the examination. Ensure that your questions are not probing for answers to the examination questions.
   - If you are found cheating, involved in discussions, talking to other students or causing any kind of disturbance during the examination, then you will be reported to appropriate University officials for violation of examination policy; you will face appropriate sanctions according to the university examination policy.
   - Answers must be properly marked in the answer book with the corresponding question number. Only answers in the answer book will be marked and graded.
   - Return both the answer/question books back to the proctor before leaving the examination hall.
   - You must stop writing when any of the proctors announces that the allotted examination duration has expired.

Part A – Multiple Choice Questions (30 Marks)

Read carefully and select the BEST answer.

1. A functional walkthrough is essential in the initial phase of an audit engagement. The walkthrough's main purpose is to:
   A. Plan substantive testing.
   B. Understand the associated business processes.
   C. Comply with auditing standards.
   D. Identify control weakness.

2. One of the following best applies to an audit charter. Which one is it?
   A. It should clearly state the audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
   B. It states the overall authority, scope and responsibilities of the planned audit.
   C. It should be dynamic and allow for frequent changes based on the changing nature of technology and the audit profession.
   D. It documents the audit procedures designed to achieve the planned audit objectives.

3. Audit sampling deals with the application of audit procedures to target less than 100% of items subject to an audit. In part, it is a means of saving on time, effort and cost. All, except one, of the following are true with respect to sampling for audit purposes:
   A. Failure to select an appropriate sample errors identified can mistakenly be extrapolated to the rest of the population.
   B. The more homogenous the population the lower the sample size needed.
   C. There is a potential chance of failing to detect some material finding.
   D. A large sample size will eliminate detection risk.

4. One of the following principles best captures the role of governance and management of enterprise IT:
   A. Ensuring optimization of resources
   B. Enablement of a holistic approach
   C. The management of organization information
   D. The management of IT operations

5. An IS auditor on conducting an IS audit of an organization's IT applications uncovers an undocumented application running on the organization's servers. This application was not included in the scope of the audit at the planning stage. The IT Manager in change of applications says that the necessary documentation is under preparation. Once ready, the approval process will commence. The auditor should as a first step do the following:
    A. Record this as a finding of control deficiency, noting that not all of the applications in the IT infrastructure has been documented.
    B. Arrange to audit the undocumented application at a different time.
    C. Conduct an assessment to determine the impact of the undocumented application.
    D. Change the scope of the audit to include the undocumented components of the network.

6. Organizations go to great lengths in implement continuous auditing to examine controls, compliance and related procedures on an ongoing basis. Continuous auditing automate the audit process with a view to obtaining results in real time. The following is a major benefit of continuous auditing:
    A. Ensures system integrity.
    B. Enforces effective preventive controls.
    C. Ensures that fraud-related activities are acted upon more quickly.
    D. Supports timely correction of errors.

7. The Plan and Organize (PO) of the Management of Enterprise IT, according to COBIT would include one of these processes?
    A. Procure IT resources
    B. Manage Operations
    C. Assess and manage IT risks
    D. Provide IT governance

8. When reviewing application development and integration controls, which of the following is least likely to be of concern to an IS auditor?
    A. Access permissions of identities spread across the different systems in the engineering ecosystem permits data modification in the test environment.
    B. The sample data used for testing and design is not fully segregated from the production version of the data.
    C. Continuous integration (CI) and continuous delivery (CD) – CI/CD - methodology does not require incorporation of application controls in the design.
    D. The testing of the application controls implementation does not consider application controls requirements to be identified in the design phase of the system's development process.

9. A forensic auditor is more likely to focus on all of the following except:
    A. Allegations of corruption and embezzlement rumoured to exist in the organization.
    B. Scrutinize manual sales entries in the books and analyze sales data.
    C. Assess transactions close to the start and end of given accounting period.
    D. Examine large transactions, new customer transactions and related parties.

10. An Information Security Management System (ISMS) is the governance structure that supports the implementation of an information security programme in an organization. ISMS is concerned with all of the following, except:
    A. Capture the tone at the top regarding information security and risk appetite.
    B. Measuring the effectiveness of technology governance and risk in the organization.
    C. The mapping of business drivers to the implementation of security controls based on risk management best practices.
    D. Roles, responsibilities and accountabilities pertaining to the information security function.

11. Which of the following would be an indicator of the effectiveness of a computer security incident response team?
    A. Number of security vulnerabilities that were patched.
    B. Percentage of business applications that are being protected.
    C. Number of successful penetration tests.
    D. Financial impact per security incident.

12. Regarding application controls, which one of the following best captures the scope of concern for an IS auditor?
    A. Access, processing and output control mechanisms.
    B. Input data, encryption methods and strength of encryption systems used.
    C. Input, processing and output controls.
    D. Identification and authentication mechanisms.

13. From a controls perspective, the main objective of classifying information assets is to:
    A. Identify which assets need to be insured against losses
    B. Establish guidelines for the level of access controls that should be assigned.
    C. Assist management and auditors in risk assessment.
    D. Ensure access controls are assigned to all information assets.

14. During a physical security audit in an organization, the auditee makes the following assertions, which were in part used to justify the acquisition of a CCTV system. Which of the statements about CCTV is not a 'fit'

    A. CCTV is a good example of an automated intrusion- detection system.

    B. CCTV is effective in deterring security violations.

    C. CCTV is aids in rapid response to security violations

    D. CCTV is a good example of a detection system.

15. A large organization has outsourced IT operations. Of the following, what should most concern an IS auditor reviewing the outsourced operation?

    A. The service provider does not have incident handling procedures.

    B. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.

    C. Recently a corrupted database could not be recovered because of library management problems.

    D. Incident logs are not being reviewed.

Part B – Short Answer Questions – 70 Marks

Answer the following questions in as few sentences as you can. Be concise with your terminology and wording.

1. (20 Marks) With respect the term 'audit' answer the following questions:
    A. Define the term ''audit'' as you understand it.
    B. Define the term IS Audit as you understand it.
    C. Describe what you understand to be the key role of audit in organizations.
    D. The audit-related concepts listed below are core to the effective execution of audits. For each of the terms, explain (a) what it means and (b) its role in the audit process:
        i. Evidence;
        ii. Due audit care;
        iii. Fair (re)presentation; and
        iv. Independence.

2. (6 Marks) Answer the following in reference to audits:
    A. Explain what you understand by the term *statutory audit*.
    B. Explain what you understand by the term *forensic audit*.
    C. Explain the major differences between the two terms.

3. (14 Marks) You have been assigned as a lead IS auditor for a large banking organization. The assignment is to audit the company's information security programme.
    A. Explain your audit strategy to execute this engagement.
    B. Describe the role of use of standards in your strategy.
    C. Develop an audit plan for the engagement and identity key players in each of the steps.
    D. (a) Identify the scope of the information you would require and the testing you would apply. (b) Explain how you would use standards in establishing the scope of your engagement.
    E. Explain the general limitations of audits. Illustrate with this specific audit assignment.

4. (8 marks) With respect to risk-based IS audit, explain the following terms; provide an example for each for purposes of illustration:
    A. Based on your understanding of the terms 'audit' and 'risk', explain what you understand by the term 'risk-based audit';
    B. Name at least two key benefits of risk-based audit;
    C. What are (name at least two) the disadvantages of risk-based audit.

5. (10 Marks) Controls: Distinguish between the following controls and, in each case, illustrate with an example:
   A. (a) Technical versus (b) non-technical versus;
   B. Show the use of (a) preventive controls versus (b) detective controls versus (c) corrective controls.

6. (6 Marks) A well-designed and effective system of internal controls can fully eliminate the risk of fraud.
   A. True or False
   B. Discuss justifying your response to (A)

7. (10 Marks) With respect to Continuous Control Monitoring and Auditing answer the following:
   A. What do you understand by the terms (a) Continuous Control Monitoring (CCM) and (b) Continuous Auditing.
   B. What are the (b) benefits (name at least two) of Continuous Control Monitoring and Auditing? (b) Name at least two disadvantages of Continuous Control Monitoring and Auditing.
   C. What are the limitations of Continuous Control Monitoring and Auditing?

8. (12 Marks) Testing is an integral component of IS auditing. Your task is to utilize both vulnerability assessment and penetration testing in support of your IS auditing engagement.
   A. Explain what you understand by the terms (a) vulnerability assessment and (b) penetration testing; ensure to clearly show the difference between the two terms.
   B. Describe at least two major benefits of penetration testing.
   C. Name and explain at least two major limitations/disadvantages of penetration testing as an IS audit support process.
   D. When would you choose penetration over vulnerability management?
   E. When would you choose vulnerability management over penetration testing?

9. (14 Marks) This question relates to project auditing.
   A. Explain why is project auditing important for IS projects?
   B. What is project risk assessment? Why is this essential to IS project audit?
   C. Explain the term 'readiness assessment of key project phases'. Why is readiness assessment essential?
   D. Define the term of 'post-implementation review' is IS project audit? What is the role of such post-implementation review?