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 using the fewest words possible to provide detailed, complete and correct responses.

B. You are required to 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 the associated difficulty.

D. This is a closed book examination and no reference materials are allowed 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 examination scripts are picked up; this also applies to cases where you finish earlier than the allotted period.
   - Ask the proctor questions that are meaningful in the examination context. 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. As an IS auditor, you have been asked to review how well the IT strategy aligns with the organization's corporate strategy. How will you best assess this?
   A. Determine whether all personnel are fully equipped with the necessary IT gadgets to perform their jobs.
   B. Evaluate the organization's IT plans to determine the degree to which they align with the overall corporate strategy.
   C. Check how efficiently and effectively users put assigned equipment to use.
   D. Establish how much excess capacity the organization has concerning its growing needs.

2. One of the following best captures the purpose of an **audit charter***?*
   A. It describes the process of performing the work described in the audit plan to achieve the audit's objectives.
   B. It formally defines the authority, scope, roles and responsibilities of the planned audit.
   C. It documents how the audit will be planned, executed, monitored, and closed.
   D. It links, to ongoing work in the organization, the audit that will be undertaken and how it will be executed, monitored and closed.

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

4. In what situation (from those given below) should an IS auditor utilize statistical sampling as opposed to judgmental (non-statistical) sampling?
   A. The auditor wishes to avoid sampling risk.
   B. The tolerable error rate cannot be determined.
   C. Generalized audit software is unavailable.

D. The probability of error must be objectively quantified.

5. On receiving an IS auditor's report, a client responds to a corrective action recommendation stating that "the problem has never occurred before," adding that "it is not the norm for the establishment's operations." Which of the following is the most appropriate action for the auditor?
   A. Revisit and discuss, in-depth, the issue with the client to evaluate the relevance of the response.
   B. Draft a response explicitly requesting a more concise root-cause analysis.
   C. Schedule a follow-up audit immediately.
   D. Note that the deficiency is the result of a random occurrence.

6. A key benefit of continuous auditing and control techniques is:
   A. Catch and correct errors in a timely fashion.
   B. Rapidly detect fraud when it happens.
   C. Effective enforcement of preventative controls
   D. Ensure system integrity.

7. The Acquire and Implement (AI) of the Management of Enterprise IT, according to COBIT would include all of the following, except:
   A. AI1 Identify automated solutions.
   B. Procure IT resources
   C. Acquire and maintain technology infrastructure
   D. Manage changes

8. Which of the following is least likely to be of concern to an IS auditor when reviewing application or system design processes for information security controls?
   A. The sample data used for testing and design is not adequately segregated from the production version of the data.
   B. The SDLC methodology does not require that security be considered as part of the design criteria.
   C. Access permissions of testing and design personnel permit data modification in the test environment.

D. The testing of the application coding does not consider the security requirements identified in the design phase of the system's development process.

9. During an IS audit, the IS auditor determines that there is a control weakness due to the lack of available standards. When developing the findings and recommendation for the audit report, which of the following items should not be considered for inclusion as reasons for improving standards in the organization?
   A. Standards creation is an industry best practice.
   B. Standards provide simplified solutions to problems, enabling leverage of fewer solutions and economies of scale.
   C. Standards provide common ground that will increase the efficiency of the operations.
   D. Standards ensure that individual policy interpretation will not result in the establishment of weaker security overall by lowering the minimum security level.

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 of the information security function.

11. While evaluating an information security programme the IS auditor establishes that industry best practices have not been followed to inform the development of the programme. Which of the following would be the <u>least important factor</u> to consider when determining the recommendation related to making changes to the programme?
   A. Whether an account of the existing controls for managing security threats has been undertaken.
   B. Whether the architectural design of the security deployed meets a state-of-the-art defence.
   C. Whether a risk assessment was part of the determination of what the program elements should be.

D. Whether the security officer had documented policies and procedures to direct the programme.

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

13. Information classification is essential for effectively protecting an organization's assets. What is the main objective of classifying information assets from the perspective of controls?
    A. Enable risk assessment for both management and auditors.
    B. Establish guidelines for the level of access controls that should be assigned.
    C. Determine which assets require to be insured against losses
    D. Ensure access controls are assigned to all information assets.

14. In examining controls on logging and monitoring network activity, the IS auditor would consider one of the following the most important associated controls.
    A. Developing exception-based reporting and log correlation processes to reduce the amount of log review required.
    B. Ensuring that the logs cannot be accessed using the systems administrator's access privileges.
    C. Having the capability to analyze the logs and take action based on the results of the analysis.
    D. To assure that forensics would be carried out accurately and hence that the information is time-synchronized for that purpose.

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

C. Incident logs are not being reviewed.

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

Part B – Short Answer Questions – 70 Marks

Answer the following questions in as few words as possible using concise terminology and wording.

1. Answer the following regarding the term 'audit' (10 marks)
    A. Define the term ''audit'' as you understand it.
    B. Define the term IS Audit as you understand it.
    C. Explain what you understand by the term *statutory audit*.
    D. Explain what you understand by the term *forensic audit*.
    E. Explain the major differences between the two terms.

2. Concerning IT Governance, explain the following terms and why they matter (8 marks)
    A. Define the term 'IT Governance'.
    B. Explain the purpose of IT Governance.
    C. Strategic alignment between IT and business.
    D. Why is the management of IT risks a concern for IT Governance?

3. Concerning risk-based IS audit, answer the following questions: explain the following terms; provide an example for each for purposes of illustration (10 Marks):
    A. Describe what you understand by the term 'risk-based audit.
    B. Explain the following terms, providing an example for each for purposes of illustration
        i. Inherent risk
        ii. Control risk
        iii. Detection risk
        iv. Overall audit risk

4. Application Controls (10 marks)
    A. Explain what you understand by the term ''Application Controls''
    B. What is the purpose of application controls as relates to IS environments?

C. Concerning application controls, explain the following terms:
   i. Input controls
   ii. Output controls
   iii. Processing controls

5. Testing is an integral component of IS auditing. Your task is to design a test plan for an organization's network infrastructure, including penetration testing. (8 marks)
   A. Define the terms black box, grey box, and white box testing.
   B. Explain the pros and cons of each of the testing approaches.
6. Computer Assisted and Auditing Techniques (CAATs) (12 marks)
   A. Explain your understanding of the term Computer Assisted and Auditing Techniques (CAATs).
   B. Why do need CAATs and hence what benefit do they provide?
   C. What are the limitations of CAATs?
   D. Develop a scenario where you would use a combination of fraud detection principles and techniques in combination with CAATs to ensure timely fraud detection.
7. This question relates to project auditing. (12 marks)
   A. Describe what you understand by the term 'project'.
   B. Explain why is project auditing important for IS projects.
   C. What is project risk assessment? Why is this essential to IS project audit?
   D. Explain the term 'readiness assessment of key project phases'. Why is readiness assessment essential?
   E. Define the term 'post-implementation review' in IS project audit. What is the role of such a post-implementation review?