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 detailed, complete and correct answers.

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 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. As an IS auditor you have been tasked to review the degree to which the IT strategy aligns with the organization's business objectives. How can you best assess this?
   A. Check how efficiently and effectively users put assigned equipment to use.
   B. Examine the organization's IT plans and programmes to determine what elements of the business strategy they support.
   C. Determine whether all personnel are fully equipped with the necessary IT tools and equipment to perform their jobs.
   D. Establish how much excess IT capacity the organization has concerning its growing needs.

2. Concerning IT Governance benefits in an organization, the IS auditor must understand that the core elements of IT Governance include Risk, Control and what else?
   A. Compliance.
   B. Transparency.
   C. Value.
   D. Regulation.

3. Information Security Audit includes assessment of all of the following, except:
   A. The organization and staffing of information security.
   B. Security of the data centre and its management.
   C. Costs associated with system & transaction controls.
   D. Incident management & contingency plans

4. An 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. Incident logs are not being reviewed.
   D. Recently a corrupted database could not be recovered because of library management problems.

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

6. Your organization's audit department processes large volumes of transactions daily and plans to implement continuous auditing and control techniques. Which of the following best captures the benefit of such a strategy?

   A. Fraud is likely to be detected promptly.
   B. Errors can be corrected in a timely fashion.
   C. System integrity is ensured.
   D. Effective preventive controls are enforced.

7. An information systems (IS) auditor would expect a defence-in-depth approach to information protection or would recommend that one be implemented for the following reasons, except:

   A. Costs can be reduced by multiple iterations of solving most of the problems at a minimal cost and then applying another economic solution to address most of the remaining exposure rather than the extensive and expensive application of one solution set.
   B. More complex security solutions can lead to higher requirements for training and related support costs including audit requirements.
   C. Security solutions never completely solve a problem and a defence-in-depth method provides opportunities to address residual risk from one solution with another solution.
   D. It provides several different security mechanisms that increase the difficulty for hackers and intruders due to the increased knowledge required for compromise.

8. In conducting a physical security audit of an organization, the auditee makes the following assertions which are part justification for the acquisition of a CCTV system. Which of the statements about CCTV is not true?

   A. CCTV is a good example of a detection system.
   B. CCTV is effective in deterring security violations.
   C. CCTV is a good example of an automated intrusion-detection system.
   D. CCTV is a good example of a deterrent system.

9. From a control perspective, the main objective of classifying information assets is to:

   A. Assist management and auditors in risk assessment.
   B. Establish guidelines for the level of access controls that should be assigned.
   C. Identify which assets need to be insured against losses.
   D. Ensure access controls are assigned to all information assets.

10. The following are the objectives of auditing an information systems (IS) project, except:

    A. Recommend corrective actions to address identified risks.
    B. Identify risks related to project management of the IS project.
    C. Promote awareness of project areas that need improvement.
    D. Establish the value the IS project would deliver to the organization.

11. Given the situations indicated below, in which one should an IS auditor utilize statistical sampling rather than judgmental (non-statistical) sampling?

    A. The auditor wishes to avoid sampling risk.
    B. The probability of error must be objectively quantified.
    C. The tolerable error rate cannot be determined.
    D. Generalized audit software is unavailable.

12. As an IS auditor, you have been asked to review your organization's IT governance practices. Which of the following BEST helps the auditor evaluate the degree of alignment between IT and the business?

    A. IT balanced scorecard (IT BSC).
    B. IT Budget
    C. Operational procedures
    D. IT policies.

13. Information Systems Audit is important in successful systems development considering that many systems fail due to all of the following, except:

    A. Alignment with corporate objectives and external environment.
    B. Poor education or low experience of employees.
    C. Poor alignment thus resulting in unrealistic expectations.
    D. Lack of or poor management support for system development.

14. It is usual for an IS auditor to conduct a functional walkthrough in the initial phase of an audit engagement. The main purpose of doing so is to:

    A. Understand the business processes.
    B. Plan substantive testing.
    C. Comply with auditing standards.
    D. Identify control weaknesses.

15. The Align, Plan and Organize (APO) of the Management of Enterprise IT, according to COBIT would include all of the following, except:

    A. Managed Strategy
    B. Managed Organizational Change
    C. Managed Budget and Costs
    D. Managed Risk

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. It is often advised that auditors take a risk-based approach to planning and conducting audits. Given that context, **explain** what you understand by the following terms, providing an example for each for purposes of illustration (12 Marks):
    A. Risk-Based Audit
    B. Inherent Risk
    C. Control Risk
    D. Detection Risk
    E. Overall Audit Risk

2. You are the lead IS auditor for a large banking organization assigned to audit the company's systems for mobile banking services. (14 marks)
    A. Explain your audit strategy to execute this engagement.
    B. Develop an audit plan for the engagement and identity of key players in each of the steps
    C. Identify the scope of the information you would require and the testing you would apply.
    D. Explain the limitations of this audit approach.

3. Control self-assessment (4 marks)
    A. Explain what you understand by the term control self-assessment.
    B. What are the key benefits of control self-assessment?

4. Computer-Aided Auditing Tools & Techniques (CAATTs) (16 marks)
    A. Explain your understanding by 'Computer-Aided Auditing Tools & Techniques – CAATTs'.
    B. Why do auditors need CAATTs? Name, at least two, benefits of using CAATTs.
    C. As useful as they are, CAATTs have limitations. Name and explain at least two of such limitations.
    D. How can CAATTs be used to support fraud risk management in an organization?

5. Answer the following briefly (8 marks):
    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.
    D. Which one of the two is superior and preferable to the other?

6. Concerning project audits, briefly explain what you understand by the terms given below, clearly indicating the objectives of the related audit and any key questions that would be part of the audit. (10 Marks)
    A. Project Risk Assessment.
    B. Readiness assessment of key project phases.
    C. Post-implementation review.
    D. Audit of key phases in the project life cycle.
    E. Overall project management methodology assessment.

7. Input Controls (10 marks)
   There are three kinds of application controls, namely, input, processing, and output.
    A. Explain what you understand by the term input controls.
    B. Why do we need input controls?
    C. Name at <u>least 2 ways</u> illustrating how input controls work.
    D. Identify the key role of input controls in an IS system.
    E. Give an example of consequences that would arise out of weak input controls.

8. Concerning Continuous Control Monitoring and Auditing answer the following (8 marks)
    A. Explain your understanding of the term Continuous Control Monitoring and Auditing.
    B. Why do need Continuous Control Monitoring and Auditing? Name at least three benefits arising from Continuous Control Monitoring and Auditing. benefit does it provide?
    C. What are the limitations of Continuous Control Monitoring and Auditing?
    D. Name and describe one practical example where CCM could be useful.

9. Testing is an integral component of IS auditing. Your task is to design a testing plan including penetration testing for an organization's network infrastructure. (12 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.

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