Title (Units): **COMP7560 Information Systems Auditing (3,3,0)**

Course Aims: To give students a thorough grounding in the theory, techniques and practical issues involved in computer-based information systems auditing.

Prerequisite: Nil

Course Intended Learning Outcomes (CILOs):
Upon successful completion of this course, students should be able to:

No.	Course Intended Learning Outcomes (CILOs)
	Knowledge
1	Illustrate and explain the fundamental concepts of information systems auditing, computer security threats and remedies
2	Identify the possible risks of information systems
3	Identify the proper controls to mitigate the risks in IT environment
	Professional Skill
4	Create IS Audit programs
5	Apply IS auditing concepts to various aspects of security controls
	Attitude
6	Develop a critical mind for evaluating and auditing information systems

Calendar Description: This course is to give students a thorough grounding in the theory, techniques and practical issues involved in computer-based information systems auditing. The students will have an in-depth understanding of auditing concepts and methods after taking this course.

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1-3	Students will attend lectures to learn the concepts of information systems auditing, computer security threats and remedies.
4-6	Students will be given case studies and participate in class discussion for in-depth learning.
4-6	Students will work on written assignments to consolidate and apply what they have learnt. They will also work on a project which involves information gathering, self-reading, critical thinking and creativity.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	40%	1-6	Continuous assessments, e.g. written assignment, and project, are designed to measure how well the students have learned the basic concepts of physical, logical and operational controls, and their understanding of different types of computer security threats and the corresponding remedies.
2	Examination	60%	1-6	Final examination questions are designed to evaluate students' understanding of the course material, and how far students have achieved the intended learning outcomes. Questions will primarily be analysis and skills based to assess the students' ability to audit and analyze the security controls of different computer systems.

Assessment Rubrics:

Excellent (A) **Good (B)** **Satisfactory (C)** **Fail (F)**

Knowledge of IS auditing	Demonstrate thorough knowledge and understanding of IS auditing	Demonstrate sufficient knowledge and understanding of IS auditing	Demonstrate some knowledge and understanding of IS auditing	Demonstrate little or no knowledge and understanding of IS auditing
Knowledge of computer security threats and remedies	Demonstrate thorough knowledge and understanding of different types of computer security threats and the corresponding remedies	Demonstrate sufficient knowledge and understanding of different types of computer security threats and the corresponding remedies	Demonstrate some knowledge and understanding of different types of computer security threats and the corresponding remedies	Demonstrate little or no knowledge and understanding of different types of computer security threats and the corresponding remedies
Organization security and controls	Demonstrate thorough knowledge of and able to identify different types of security controls in organizations	Demonstrate sufficient knowledge of and able to identify different types of security controls in organizations	Demonstrate some knowledge of and able to identify some types of security controls in organizations	Demonstrate little or no knowledge of and unable to identify any types of security controls in organizations
Computer related controls	Demonstrate thorough knowledge and understanding of different types of computer related controls	Demonstrate sufficient knowledge and understanding of different types of computer related controls	Demonstrate some knowledge and understanding of different types of computer related controls	Demonstrate little or no knowledge and understanding of different types of computer related controls
IS audit programs	Demonstrate high ability of evaluating and auditing information systems and creating IS audit programs	Demonstrate sufficient ability of evaluating and auditing information systems and creating IS audit programs	Demonstrate some ability of evaluating and auditing information systems and creating IS audit programs	Unable to evaluate and audit information systems and create IS audit programs

Course Content and CILOs Mapping:

Content		**CILO No.**
I	Introduction to Information Systems Auditing	1,4,6
II	Organization Security and Controls	2,5,6
III	Application Software Control	1,2,5,6
IV	Database Controls	1,2,5,6
V	Network Security and Controls	1,2,5,6
VI	Advanced Topics/Case Studies	3,6

References:

- A. R. Otero, Information Technology Control and Audit, 5th Edition, CRC Press, 2019.
- C. Davis, M. Schiller, and K. Wheeler, IT Auditing: Using Controls to Protect Information Assets, McGraw-Hill, 2011.
- J. A. Hall, Information Technology Auditing, 4th Edition, Cengage Learning, 2016.
- J. E. Hunton, S. M. Bryant, N. A. Bagranoff, Core Concepts of Information Technology Auditing, Wiley, 2003
- J. J. Champlain, Auditing Information Systems, 2nd Edition, Wiley, 2004.
- M. Kegerreis, M. Schiller, and C. Davis, IT Auditing Using Controls to Protect Information Assets, 3rd Edition, McGraw-Hill, 2020.

- R. Johnson, M. Weiss, and Michael G. Solomon. Auditing IT Infrastructures for Compliance with Cloud Labs, 3th Edition. Jones & Bartlett Learning, 2023.
- S. Senft, F. Gallegos, and A. Davis, Information Technology Control and Audit, CRC Press, 2013.
- V. Hingarh and A. Ahmed, Understanding and Conducting Information Systems Auditing, John Wiley & Sons, 2013.
- V. Raval, and A. Fichadia, Risks, Controls and Security: Concepts and Applications, Wiley, 2007.
- Selected articles from Information Systems Control Journal.

Course Content:

Topic

I. Introduction to Information Systems Auditing
   A. Objectives of IS audit and control
   B. The structure of an IS audit and audit reports
   C. Types of internal controls
   D. IS auditing standards
   E. IT Governance

II. Organization Security and Controls
   A. Physical security controls
   B. Logical security controls
   C. Operating controls
   D. Personnel security and management practices

III. Application Software Control
   A. Software development control
   B. Input control
   C. Processing control
   D. Output control
   E. Documentation control
   F. Computer assisted audit tools

IV. Database Controls
   A. Access controls
   B. Inference controls
   C. Encryption controls
   D. Backup controls

V. Network Security and Controls
   A. Intranet Risks
   B. Internet Risks
   C. Controls related to EDI, E-mail, On-line Transactions

VI. Advanced Topics/Case Studies