Title (Units): **COMP4046 Information Systems Control and Auditing (3,3,0)**

Course Aims: This course aims to give students a thorough grounding in the theory, techniques and practical issues involved in computer-based information systems control and auditing. The contents of this course include (but not limited to) concepts, approaches, and techniques of information system auditing, security controls in organizations, and the application of IT in auditing. This course reviews some basic concepts of computer security.

Prerequisite: COMP3015 Data Communications and Networking

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 the fundamental concepts of information systems auditing and IT application in auditing
2	Identify the security controls in organization
3	Explain the basic concepts of computer security, computer security threats and the corresponding remedies
4	Describe the trend of computer security threats
	Professional Skill
5	Apply physical, logical and operational security controls
6	Assess the security of computer systems in terms of how well they are protected from computer security threats and integrate computer security mechanisms to protect computer systems from security threats

Calendar Description: This course provides the theory, techniques and practical issues relate to computer-based information systems control and auditing. Students will learn the concepts, approaches, and techniques to carry out information system auditing and security controls in organizations.

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1-4	Students will attend lectures for the concepts of IT auditing, security threats and controls.
1-6	Students will be provided with examples and cases to illustrate the topics covered.
5, 6	Students will work on exercises and assignments to consolidate their understanding on the covered topics.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	40%	1-6	Continuous assessments, e.g. a written assignment and a project will be designed to measure how well students have learned the basic concepts of physical, logical & 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. Examination may include analysis and skills based questions to assess the students' ability to audit and analyze the security controls of different computer systems.

Assessment Rubrics:

	Excellent (A)	Good (B)	Satisfactory (C)	Marginal Pass (D)	Fail (F)
Concepts of information systems auditing	Show thorough understanding of information systems auditing concepts	Show good understanding of information systems auditing concepts	Show sufficient understanding of information systems auditing concepts	Show limited understanding of information systems auditing concepts	Show little or no understanding of information systems auditing concepts
Security controls in organization	Show thorough understanding of security controls in organization	Show good understanding of security controls in organization	Show sufficient understanding of security controls in organization	Show limited understanding of security controls in organization	Show little or no understanding of security controls in organization
Computer security concepts	Demonstrate thorough understanding of basic concepts of computer security	Demonstrate good understanding of basic concepts of computer security	Demonstrate sufficient understanding of basic concepts of computer security	Demonstrate limited understanding of basic concepts of computer security	Demonstrate little or no understanding of basic concepts of computer security
Computer security threats and the corresponding remedies	Demonstrate thorough understanding of computer security threats and the corresponding remedies	Demonstrate good understanding of computer security threats and the corresponding remedies	Demonstrate sufficient understanding of computer security threats and the corresponding remedies	Demonstrate limited understanding of computer security threats and the corresponding remedies	Demonstrate little or no understanding of computer security threats and the corresponding remedies
Trend of computer security threats	Able to describe trend of computer security threats, with thorough justification	Able to describe trend of computer security threats, with good justification	Able to describe some trend of computer security threats, with sufficient justification	Able to describe trend of computer security threats, with limited justification	Not able to describe trend of computer security threats

Course Content and CILOs Mapping:

Content		CILO No.
I	Introduction to IS Auditing	1
II	Organization Security Controls	2, 5
III	Systems and Network Security	3, 4, 6
IV	Incident Handling and Computer Forensic	6

References:

- B. Nelson, A. Phillips and C. Steuart, Guide to Computer Forensics and Investigations (5th Edition), Cengage Learning, 2016.
- H. James, T. Singleton, Information Systems Auditing and Assurance (2nd Edition), Cengage Learning, 2004.
- C. P. Pfleeger, S. L. Pfleeger and J. Margulies, Security in Computing (5th Edition), Prentice Hall, 2015
- W. Stallings, Cryptography and Network Security: Principles and Practice (6th Edition), Pearson, 2014.
- British Standard BS 7799-1:1999 (Part 1 & 2).
- M. Bishop, Introduction to Computer Security, Addison-Wesley, 2005.
- P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide, International Journal of Computer Research, Volume 20, Issue 4, 2013

- P. Mell, K. Kent and J. Nusbaum, NIST SP800-83 − Guide to Malware Incident Prevention and Handling, NIST, November 2005.
- K. Omoteso, Audit Effectiveness: Meeting the IT Challenge. Gower Publishing, 2013.
- R. Argiento, Introduction to Computer Security, Pearson, 2013.
- 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.

Course Content:

Topic

I. Introduction to IS Auditing
   A. Objectives of IS audit and control
   B. The structure of an IS audit and audit reports
   C. IS auditing standards
   D. Computer assisted audit tools

II. Organization Security Controls
   A. Physical controls
   B. Logical controls
   C. Operational controls
   D. Personnel security and management practices
   E. Application software control

III. Systems and Network Security
   A. Systems and network security issues
   B. Non-malicious errors, virus and worms
   C. Access control, trusted operating systems
   D. Encryption in network
   E. User authentication
   F. E-mail security
   G. IP security
   H. Web security

IV. Incident Handling and Computer Forensic