Title (Units): COMP7330 Information Systems Security & Auditing (3,3,0)

Course Aims: To introduce the fundamental concepts and techniques in computer and network security, giving students an overview of information security and auditing, and to expose students to the latest trend of computer attack and defense. Other advanced topics on information security such as mobile computing security, security and privacy of cloud computing, as well as secure information system development will also be discussed.

Prerequisite: Postgraduate Student Standing

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

No.	Course Intended Learning Outcomes (CILOs)
	Knowledge
1	Describe fundamental concepts of information security and systems auditing
2	Analyze the latest trend of computer security threats and defense
	Professional Skill
3	Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms
4	Explain the security controls in the aspects of physical, logical and operational security control
	Attitude
5	Critically evaluate the security of information systems

Calendar Description: This course aims to introduce students to the fundamental concepts and techniques in computer and network security, and giving students an overview of information security and auditing, and to expose students to the latest trend of computer attack and defense. Other advanced topics on information security such as mobile computing security, security and privacy of cloud computing, as well as secure information system development will also be discussed.

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1-2	Students will learn various information security & auditing concepts, and technologies via lectures and assignments.
3-5	Students will investigate various information security and auditing related topics through projects and assignments.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	40%	1-5	Continuous assessments are designed to measure how well the students have learned the material. Projects and/or assignments are designed to give students hands-on experience in the subject matter.
2	Examination	60%	1-4	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 analyze the security of different computer systems.

Assessment Rubrics:

Excellent (A)	• Achieve the five CILOs, demonstrating a good mastery of both the theoretical and practical aspects of information security & system auditing • Have a solid understanding of information security & system auditing fundamental concepts, and be able to explain and highlight the key points of these concepts • Able to comprehend and have a sound knowledge of the latest trend of computer security technologies, threats and defense • Able to conduct security analysis and auditing on computer systems, and possibly highlighting security vulnerabilities with detailed explanation and proper reasoning • Demonstrating a good mastery of explaining the security controls in the aspects of physical, logical and operational security control • Able to recommend suitable computer security mechanisms to different situations and computing environments, and be able to design and develop, with competence, high quality computer security systems using these technologies
Good (B)	• Achieve the five CILOs, demonstrating a good understanding of both the theoretical and practical aspects of information security & system auditing • Have a good understanding of information security & system auditing fundamental concepts • Able to comprehend and have a basic understanding of the latest trend of computer security technologies, threats and defense • Able to conduct security analysis and auditing on computer systems with sound reasoning • Able to explain the security controls in the aspects of physical, logical and operational security control • Able to apply computer security mechanisms to different situations and computing environments, and be able to design and develop computer security systems using these technologies
Satisfactory (C)	• Achieve most of the five CILOs, demonstrating a basic level of understanding of the theoretical and practical aspects of information security & system auditing • Have a basic understanding of information security & system auditing fundamental concepts • Barely understand the latest trend of computer security technologies, threats and defense • Able to conduct a basic security analysis and auditing on most computer systems • At an acceptable level, be able to explain the security controls in the aspects of physical, logical and operational security control • Demonstrate an adequate level of ability of applying computer security mechanisms to different situations and computing environments
Fail (F)	• Achieve less than three of the five CILOs, and have little understanding of the theoretical and practical aspects of information security & system auditing • Unable to provide solutions to simple problems which require basic understanding of information security & system auditing fundamental concepts • Unable to understand the latest trend of new computer security technologies, threats and defense • Unable to conduct security analysis or auditing on computer systems • Unable to explain the security controls in the aspects of physical, logical and operational security control • Have little understanding of computer security mechanisms and have difficulty in applying these technologies to computing environments

Course Content and CILOs Mapping:

Content		CILO No.
I	Introduction to Information Security and IS Auditing	1,4,5
II	Organization Security and Controls	1,4,5
III	Basics of Information Security	1,2
IV	Basics of Cryptographic Technologies	1,2

V	User Authentication, Access Control and Identity Management	1,2
VI	Host Security – Attack & Defense	2,3,5
VII	Network Security – Attack & Defense	2,3,5
VIII	Information System Security Auditing, Computer Forensic and Other Security Technologies	2,5

References:

- William Stallings and Lawrie Brown, Computer Security Principles and Practice, (3rd Edition), Pearson, 2014
- Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 2015
- Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno,Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010.
- Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Software Security Engineering: A Guide for Project Managers, Addison-Wesley, 2008.
- Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006.
- Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley, 2008.
- Eric Cole, Network Security Bible, 2nd Edition, Wiley, 2009.
- Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations (with DVD) (5th Edition), Course Technology, 2016.
- Michael E. Whitman, Herbert J. Mattord, Management of Information Security, 5th Edition, Course Technology, 2016.
- Michael E. Whitman, Herbert J. Mattord, Readings and Cases in the Management of Information Security, 3rd Edition, Course Technology, 2005.
- H. James, Tommie Singleton, Information Systems Auditing and Assurance (2nd Edition), Cengage Learning, 2004.
- R. Weber, Information Systems Control and Audit, Prentice Hall, 1999.
- J. J. Champlain, Auditing Information Systems - A Comprehensive Reference Guide, John Wiley & Sons Inc, 2003
- J. A. Hall, Information Technology Auditing and Assurance, 4th Edition, Cengage Learning, 2011.
- K. Omoteso, Audit Effectiveness: Meeting the IT Challenge. Gower Publishing, 2013.
- 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.
- British Standard BS 7799-1:1999 (Part 1 & 2).
- ISO/IEC 27001:2013
- Information Security Management Handbook, 4th Edition (2001), Vol. 2.
- Information Security Management Handbook, 4th Edition (2002), Vol. 3.
- Information Security Management Handbook, 5th Edition (2004), Vol. 1.
- R. O'Hanley and J.S. Tiller, Information Security Management Handbook, 6th Edition, Volume 7, 2013.
- T. Grance, K. Kent & B. Kim, NIST SP800-61 – Computer Security Incident Handling Guide, NIST, 2004.
- P. Mell, K. Kent & J. Nusbaum, NIST SP800-83 – Guide to Malware Incident Prevention and Handling, NIST, November 2005.
- K. Kent, S. Chevalier, T. Grance, & H. Dang, NIST SP800-86 – Guide to Integrating Forensic Techniques into Incident Response, NIST, August 2006.
- NIST SP800-12, An Introduction to Computer Security: The NIST Handbook, NIST, 1995.

Course Content:

<u>Topic</u>

I. Introduction to Information Security and 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 and Controls

A. Physical security controls
- contingency plan, disaster recovery and reconstruction

B. Logical security controls
- operating system security and access control

C. Operating controls
- segregation of duties, monitoring and logging controls

D. Personnel security and management practices
- user training and incident reporting
- third-party access and outsourcing

E. Application software control
- software development control
- input, processing and output control

III. Basics of Information Security

IV. Basics of Cryptographic Technologies

A. Symmetric encryption

B. Asymmetric encryption

C. Basics of message authentication and cryptographic hash functions

D. Digital signatures and digital certificates

E. Public-key Infrastructure & Web of Trust

V. User Authentication, Access Control and Identity Management

VI. Host Security – Attack & Defense

A. Virus

B. Worm

C. Trojan Horse

D. Rootkit & Stealth

E. Stack-based Buffer Overflow

VII. Network Security – Attack & Defense

A. Network Attacks
- Host based attacks
- Network attacks
- Web based attacks

B. Network Defense
- Intrusion detection systems & firewall
- IPSec and DNSSec
- IPv6
- Cloud computing

VIII. Information System Security Auditing, Computer Forensic and Other Security Technologies

A. Security auditing and security standards

B. Incident handling and computer forensic

C. Other security technologies including blockchain