City University of Hong Kong
Course Syllabus

offered by Department of Information Systems
with effect from Semester A in 2017 / 2018

Part I Course Overview

Course Title:	Information Systems Audit
Course Code:	IS4537
Course Duration:	One Semester (13 weeks)
Credit Units:	3
Level:	B4
Proposed Area: *(for GE courses only)*	☐ Arts and Humanities ☐ Study of Societies, Social and Business Organisations ☐ Science and Technology
Medium of Instruction:	English
Medium of Assessment:	English
Prerequisites: *(Course Code and Title)*	Nil
Precursors: *(Course Code and Title)*	Nil
Equivalent Courses: *(Course Code and Title)*	IS4501 Information Systems Audit
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

(A 150-word description about the course)

Information security has become more and more important in today's business world. From time to time there are threats and vulnerabilities facing us. This course has been designed to teach us the nature of such threats and vulnerabilities to information processes so that we can know our enemies and the related technical and managerial solutions for us to counteract with. Besides, through learning the key activities and techniques in performing risk management and information systems control we can know ourselves. To make sure the technical controls and management controls are well designed and functioning properly, role of information systems audit is explained in enhancing asset safeguarding, data integrity, system effectiveness and system efficiency. The other goal of this course is to prepare students in achieving professional qualification as Certified Information Systems Auditor (CISA).

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs[#]	Weighting* (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Demonstrate the knowledge of information systems risk management to assess and manage risks in organizations.	25%		✓	✓
2.	Understand the technical nature of information systems threats and the technical and managerial solutions to manage them.	25%		✓	
3.	Evaluate and examine innovative controls relating to business processes and using different control objectives, activities and metrics to monitor and maintenance.	20%		✓	✓
4.	Apply appropriate techniques to handle the information systems audit life cycle and the main types of information systems audit.	20%		✓	✓
5.	Understand the professional code of ethics of the Information Systems Audit and Control Association.	10%	✓		
** If weighting is assigned to CILOs, they should add up to 100%.*		100%			

[#] Please specify the alignment of CILOs to the Gateway Education Programme Intended Learning outcomes (PILOs) in Section A of Annex.

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to self-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

TLA	Brief Description	CILO No.					Hours/week (if applicable)
		1	2	3	4	5	
TLA1: Lecture	The following items form the content of the lecture: • IS audit overview: IS security threats, audit purpose and personnel • Key concepts of IS security management • Information technology risks management • IS audit life cycle and main types of IS audit • IS audit concepts and techniques, including Computer Assisted Audit Tools and Techniques (CAATTS) • Legal and ethical issues for IT auditors	✓	✓	✓	✓	✓	Seminar: 3 Hours/Week
TLA2: Laboratory	During laboratory sessions, the following activities are used to reinforce the concepts learnt in lectures: • *Exercises*: in form of multiple choice questions, short questions, cases or article readings of the related subjects. There will also be individual exercise on CAATTS. • *Group Discussion*: group discussions in the laboratory aim to cultivate critical thinking and application of the concepts to the actual business scenarios.	✓	✓	✓	✓	✓	

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

Assessment Tasks/Activities	CILO No.					Weighting*	Remarks#
	1	2	3	4	5		
Continuous Assessment: 50%							
AT1: Continuous Assessment It consists of attendance and class participation. Each tutorial consists of exercises and group discussions to assess students' understanding of the topics and their abilities to apply their knowledge and skills.	✓	✓	✓	✓	✓	20%	
AT2: Mid-Term Test A written mid-term test is developed to assess student's competence level in the middle of the semester.	✓	✓				15%	
AT3: Project Each student will participate in group project (about 4 students per group) and work on a IS security / audit analysis report. Each group will be required to submit a project paper of detailed findings and recommendations and provide a 20-minute presentation. This allows students to apply security management concepts and methodology to identify IT risks in an organisation and provide resolutions.	✓	✓	✓			15%	
Examination: 50% (duration: one 2-hour exam)							
AT4: Final Examination A written examination is developed to assess student's competence level of the taught subjects.	✓	✓	✓	✓	✓	50%	
** The weightings should add up to 100%.*						100%	

Remark: Students must pass BOTH coursework and examination in order to get an overall pass in this course.

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Assessment Task (AT)	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
AT1: Continuous Assessment	Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to accurately assess IS audit techniques to IS audit life cycle and main types of IS audit.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to accurately apply ISACA professional code of ethics and project management techniques.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT2: Mid-Term Test	Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT3: Project	Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT4: Final Examination	Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to accurately assess IS audit techniques to IS audit life cycle and main types of IS audit.	High	Significant	Moderate	Basic	Not even reaching marginal levels

	Ability to accurately apply ISACA professional code of ethics and project management techniques.	High	Significant	Moderate	Basic	Not even reaching marginal levels

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

(An indication of the key topics of the course.)

Information Systems auditing; IT Governance; Information Technology risk management; Information Systems risk control; Information System audit process; Information Systems audit techniques; Information Systems audit life cycle; Legal and ethical issues for Information Technology Auditors.

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

1.	Hunton, J., Bryant, S. and Bagranoff, N., Core Concepts of Information Technology Auditing, Wiley & Sons. ISBN: 0471222933.

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

1.	Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 5th edition, Boston, Mass; [London]: Thomson Course Technology, 2011. ISBN: 1285448367.
2.	David L. Cannon, CISA: Certified Information Systems Auditor Study Guide, 4th edition, Indianapolis, IN: Wiley Publishing, Inc, 2011. ISBN: 9781119056249.
3.	Dhillon, Gurpreet, Principles of Information Systems Security: Texts and Cases, John Wiley, 2007. ISBN: 978-0-471-45056-6.
4.	James A. Hall, Tommie Singleton, Information Technology Auditing, 3rd edition, South-Western, Cengage Learning, 2005. ISBN: 1439079110.
5.	Weber, Ron, Information Systems Control and Audit, Prentice-Hall, Inc, 1999. ISBN: 0139478701.
6.	CISA Review Manual, Information Systems Audit and Control Association, current year.
7.	Selected readings from: Computers and Security; ISACA Journal

2.3 Other Resources:

Selected readings from: Computers and Security; ISACA Journal