City University of Hong Kong
Course Syllabus

offered by Department of Information Systems
with effect from Semester A 2020/21

Part I Course Overview

Course Title:	Information Systems Infrastructure and Security Management
Course Code:	IS6526P
Course Duration:	Intensive mode: 3 days
Credit Units:	1.5
Level:	P6
Medium of Instruction:	Putonghua supplemented by English
Medium of Assessment:	Chinese
Prerequisites: *(Course Code and Title)*	Nil
Precursors: *(Course Code and Title)*	Nil
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

The aim of this course is to examine key infrastructural and security issues involved in Electronic Commerce transactions. A managerial perspective will be adopted throughout. Both electronic payment infrastructure and transactional security infrastructure will be covered.

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.	Apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	20%			
2.	Evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	20%	✓	✓	
3.	Apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	30%	✓	✓	
4.	Evaluate security of electronic payment infra-structures for Electronic Commerce.	20%			
5.	Communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.	10%			
		100%			

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: • Threats understanding and security attacking methods • Key concepts of IS security principles and tools • Information technology risks management • IS audit life cycle and IS audit controls framework • Electronic payment infrastructure • Security management and policy • Legal and ethical issues	✓	✓	✓	✓	✓	
TLA2: Class Activity	In the seminars, the following activities are used to reinforce the concepts learnt in lectures: • *Exercises:* In form of short questions, cases or article readings of the related subjects for students to have the application of concepts and theories learned in the class to the real world. • *Group Discussion:* group discussions aiming 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: Class Activity It consists of class exercises and discussion. Each class activity consists of exercises and group discussions to assess students' understanding of the topics and their abilities to apply their knowledge and skills.	✓	✓	✓	✓	✓	5%	
AT2: Individual Assignment Each student is required on the new developments related to an existing topic to give critical analysis and solution or impact to the business organizations. A written report will be used to assess student's competence level in the understanding of new developments based on the foundations of relevant topic.	✓	✓	✓	✓		15%	
AT3: Project Each student will participate in group project (about 4 to 6 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 make a 20-minute presentation. A well-written report is required to let students demonstrate their ability in applying all the concepts and theories learned in the course to provide a workable solution and consultancy to the business organizations.	✓	✓	✓	✓	✓	30%	
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%	
						100%	

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	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
AT1: Class Activity	Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to evaluate security of electronic payment infra-structures for Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to communicate effectively with the stakeholders to provide appropriate security solutions/ consultancy to the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT2: Individual Assignment	Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels

	Capability to evaluate security of electronic payment infra- structures for Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT3: Project	Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to collaboratively evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to collaboratively evaluate security of electronic payment infra-structures for Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT4: Final Examination	Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to evaluate security of electronic payment infra-structures for Electronic Commerce.	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.)

IS Auditing; IS Security Management Practices; Information Technology Risks Management; Controls Framework; Electronic Payment Systems and Infrastructure; Security Policy; Threats; Attacking Methods; Security Principles and Tools; Network Security.

Details:

- Privacy and Security Principles: Data and transactional security, data privacy, overview of privacy and security technologies – public key encryption, digital signature.
- Network security: types of security breach, general attack methods, intrusion detection system, firewall, identity threat management.
- Electronic Payment Systems: technology overview, digital cash, electronic cheques, on-line credit cards, stored value cards, on-line electronic fund transfer and debit cards, payment settlement systems and protocols.
- Certification Authorities: technology and organizational overview, formation, role, code of practice for recognised certification authorities in HKSAR.
- System Control and Audit: overview of information systems audit principles, management control, application control, evidence collection and evaluation.
- System Security Management: roles and functions, risk assessment, security strategies and policies, implementation issues, critical success factors.
- Legal and Professional issues: professional code of conduct, overview of laws relating to computer crimes, on-line transactions, intellectual property and data privacy.

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. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Course Technology, 5th edition (November 18, 2014). ISBN: 978-1285448367

2.2 Additional Readings

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

1. Greenstein Marilyn, Vasarhelyi Miklos, Electronic Commerce: Security, Risk Management and Control, 2nd edition, 2002, McGraw Hill. ISBN: 0072410817
2. Michael E. Whitman, Herbert J. Mattord, Management of Information Security, Thomson Course Technology, 2008. ISBN: 1423901304
3. Conklin, et. al, Principles of Computer Security, 2005, McGraw Hill. ISBN: 0071245006
4. Hunton, J., Bryan, S. and Bagranoff, N., Core Concepts of Information Technology Auditing, 2004, Wiley & Sons
5. Weber, Ron, Information Systems Control and Audit, 1999, Prentice-Hall, Inc. ISBN: 0139478701
6. Krause Micki, Tipton Harold, Handbook of Information Security Management, Auerbach, 1999. ISBN: 0849399742
7. Champlain Jack, Auditing Information Systems: A Comprehensive Reference Guide, 1998, John Wiley. ISBN: 0471168904

2.3 Other Resources

Selected readings from: Computers and Security; ISACA Journal