Form 2B

City University of Hong Kong

Information on a Course
offered by Department of Information Systems
with effect from Semester A in 2009 /2010

Part I

Course Title:	Infrastructure and Security Management for eCommerce
Course Code:	IS6522
Course Duration:	One Semester (13 weeks)
No. of Credit Units:	Three
Level:	P6
Medium of Instruction:	English
Prerequisites:	Nil
Precursors:	Nil
Equivalent Courses:	IS6523 Information Systems Infrastructure and Security Management
Exclusive Courses:	IS6523 Information Systems Infrastructure and Security Management

Part II

1. Course Aims:

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)

Upon successful completion of this course, students should be able to:

No.	CILOs	Weighting (if applicable)
1.	Apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	2
2.	Evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	2
3.	Apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	3
4.	Evaluate security of electronic payment infra-structures for Electronic Commerce.	2
5.	Communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.	1

3. Teaching and learning Activities (TLAs)

(designed to facilitate students' achievement of the CILOs)

Indicative of likely activities and tasks students will undertake to learn in this course. Final details will be provided to students in their first week of attendance in this course.

Seminar: 39 hours

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.

ILO No	TLA1: Lecture	TLA2: Class Activity	Hours/week (if applicable)
CILO 1	2	2	---
CILO 2	2	2	---
CILO 3	2	2	---
CILO 4	2	2	---
CILO 5	1	1	---

(1: Minor focus on the ILO; 2: Main focus on the ILO)

4. Assessment Tasks/Activities

(designed to assess how well the students achieve the CILOs)

Indicative of likely activities and tasks students will undertake to learn in this course. Final details will be provided to students in their first week of attendance in this course.

AT1: Class Activity (5%)

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.

AT2: Individual Assignment (15%)

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.

AT3: Project (30%)

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.

AT4: Final Examination (50%) – one 2-hr exam

A written examination is developed to assess student's competence level of the taught subjects.

** Students must pass both coursework and exam in order to secure an overall pass in this course. **

ILO No	AT1: Class Activity (5%)	AT2: Individual Assignment (15%)	AT3: Project (30%)	AT4: Final Exam (50%)	Remarks
CILO 1	2	1	2	2	1: Minor focus on the ILO; 2: Main focus on the ILO)
CILO 2	2	1	2	2	
CILO 3	2	2	2	2	
CILO 4	2	1	2	2	
CILO 5	1		1		

5. **Grading of Student Achievement:** Refer to Grading of Courses in the Academic Regulations for Taught Postgraduate Degrees.

ILO	Excellent	Good	Adequate	Marginal
CILO1	Effectively apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	Accurately apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	Moderately apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.	Apply some key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.
CILO2	Effectively evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	Accurately evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	Moderately evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.	Evaluate some different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.
CILO3	Effectively apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	Accurately apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	Moderately apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.	Minimally apply good security management principles and key legal issues involved in Electronic Commerce in the design of security policies and operation within organizations.
CILO4	Effectively evaluate security of electronic payment infra-structures for Electronic Commerce.	Accurately evaluate security of electronic payment infra-structures for Electronic Commerce.	Moderately evaluate security of electronic payment infra-structures for Electronic Commerce.	Minimally evaluate security of electronic payment infra-structures for Electronic Commerce.
CILO5	Extensively demonstrate effective communication skills and provide appropriate security solutions / consultancy to the business organizations.	Demonstrate some effective communication skills and provide appropriate security solutions / consultancy to the business organizations.	Demonstrate the basic communication skills and provide appropriate security solutions / consultancy to the business organizations.	Minimally demonstrate some communication skills and provide appropriate security solutions / consultancy to the business organizations.

Part III

Keyword Syllabus:

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.

Detailed Syllabus:

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.

Required Reading:

Greenstein Marilyn, Vasarhelyi Miklos, Electronic Commerce: Security, Risk Management, and Control, 2nd edition, 2002, McGraw Hill. ISBN: 0072410817

Recommended Readings:

Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Thomson Course Technology, 2009. ISBN: 1423901770

Michael E. Whitman, Herbert J. Mattord, Management of Information Security, Thomson Course Technology, 2008. ISBN: 1423901304

Conklin, et. al, Principles of Computer Security, 2005, McGraw Hill. ISBN: 0071245006

Hunton, J., Bryan, S. and Bagranoff, N., Core Concepts of Information Technology Auditing, 2004, Wiley & Sons

Weber, Ron, Information Systems Control and Audit, 1999, Prentice-Hall, Inc. ISBN: 0139478701

Krause Micki, Tipton Harold, Handbook of Information Security Management, Auerbach, 1999. ISBN: 0849399742

Champlain Jack, Auditing Information Systems: A Comprehensive Reference Guide, 1998, John Wiley. ISBN: 0471168904

Selected readings from: Computers and Security; ISACA Journal