IS6523: INFORMATION SYSTEMS INFRASTRUCTURE AND SECURITY MANAGEMENT

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Information Systems Infrastructure and Security Management

Subject Code
IS - Information Systems
Course Number
6523

Academic Unit
Information Systems (IS)

College/School
College of Business (CB)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
Nil

Equivalent Courses
IS6522 Infrastructure and Security Management for eCommerce

Exclusive Courses
Nil

Part II Course Details

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.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-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	x	x	
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	x	x	
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			

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 real-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.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	LTA1: Lecture	Students will learn the following items from 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	1, 2, 3, 4, 5	
2	LTA2: Class Activity	Students will be able to reinforce the concepts learnt in lectures through the following activities in the seminars: - 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.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	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.	1, 2, 3, 4, 5	5	-	Yes
2	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.	1, 2, 3, 4, 5	15	-	Yes

3	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.	1, 2, 3, 4, 5	30	-	Yes

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Minimum Continuous Assessment Passing Requirement (%)

25

Minimum Examination Passing Requirement (%)

25

Additional Information for ATs

AT4: Final Examination
A written examination is developed to assess student's competence level of the taught subjects.

Assessment Rubrics (AR)

Assessment Task

AT1: Class Activity (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT1: Class Activity (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT1: Class Activity (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

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.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT1: Class Activity (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to evaluate security of electronic payment infra- structures for Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT1: Class Activity (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT2: Individual Assignment (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT2: Individual Assignment (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT2: Individual Assignment (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

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.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT2: Individual Assignment (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to evaluate security of electronic payment infra- structures for Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to collaboratively evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
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.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to collaboratively evaluate security of electronic payment infra-structures for Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
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.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capability to evaluate security of electronic payment infrastructures for Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT1: Class Activity (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT1: Class Activity (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT1: Class Activity (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

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.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT1: Class Activity (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Capability to evaluate security of electronic payment infrastructures for Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT1: Class Activity (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT2: Individual Assignment (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT2: Individual Assignment (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT2: Individual Assignment (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
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.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT2: Individual Assignment (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Capability to evaluate security of electronic payment infra- structures for Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT3: Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT3: Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Capability to collaboratively evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT3: Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

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.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT3: Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Capability to collaboratively evaluate security of electronic payment infra-structures for Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT3: Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to communicate effectively with the stakeholders to provide appropriate security solutions / consultancy to the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Assessment Task

AT4: Final Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to apply key security technical concepts and tools and the IT risks management to identify and counteract possible threats facing the business organizations.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Capability to evaluate different types of audit principles, controls framework, evidence collection and evaluation techniques in the context of Electronic Commerce.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
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.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Not even reaching marginal levels

Assessment Task
AT4: Final Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Capability to evaluate security of electronic payment infra- structures for Electronic Commerce.

Excellent

(A+, A, A-) High

Good

(B+, B) Moderate

Marginal

(B-, C+, C) Basic

Failure

(F) Not even reaching marginal levels

Part III Other Information

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.
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.

Reading List

Compulsory Readings

	Title
1	Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Course Technology, 6th edition. ISBN: 978-1337102063

Additional Readings

	Title
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
8	Selected readings from: Computers and Security; ISACA Journal