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:	Risk Management and Information Systems Control
Course Code:	IS4543
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)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

(A 150-word description about the course)

This course aims to identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy; develop and implement risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives; monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy; design and implement information systems controls in alignment with the organization's risk appetite and tolerance levels to support business objectives; monitor and maintain information systems controls to ensure they function effectively and efficiently; and achieve professional qualification as Certified in Risk and Information Systems Control (CRISC).

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.	Examine the standards, frameworks and leading practices related to identifying, assessing, evaluating, responding to and monitoring information systems risk.	30%	✓	✓	
2.	Explain the nature of threats and vulnerabilities to information processes and related security concepts; and how effective technical and managerial solutions can be devised.	30%	✓		✓
3.	Identify the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.	20%		✓	✓
4.	Apply the concepts and techniques learnt on risk management in real-life scenarios.	20%		✓	✓
	** 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.)

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.

TLA	Brief Description	CILO No.				Hours/week (if applicable)
		1	2	3	4	
TLA1. Lecture	Risk IT framework and the key concepts of risk governance, risk evaluation, risk response are explained by instructor using examples and cases. Students practice the techniques in design, implement, monitor and maintain risk-based, efficient and effective information systems controls with in-class discussions and activities.	✓	✓	✓		Seminar: 3 hrs/week
TLA2. Tutorial	During tutorial sessions, the following activities are used to reinforce the concepts learnt in lectures: • *Case Studies*: real-life simulated cases will be provided as the basis for discussion. • *Group Discussion*: group discussions aim to cultivate critical thinking and application of the concepts to the actual business scenarios. • *Exercises*: can be in the form of quizzes, multiple choice questions, short questions, cases or article readings on the related topics.	✓	✓	✓	✓	

4. Assessment Tasks/Activities (ATs)

(ATs are 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.

Assessment Tasks/Activities	CILO No.				Weighting *	Remarks
	1	2	3	4		
Continuous Assessment: 50%						
AT1. Continuous Assessment: Students are assessed based on their participation in classes, tutorials and discussions. There will be in-class exercises, assignments and presentations to assess students' progress and understanding of the topics and their abilities to apply the knowledge and skills.		✓	✓	✓	20%	

AT2. Project: Each student will participate in a group to work through the risk management life cycle. The group will be asked to provide a report with the risk assessment results and recommendations. They also need to have a face-to-face meeting with the company management to present such findings and recommendations and address management's concerns in the meeting. This allows students to apply risk and security management concepts and methodology to critically identify and respond to information systems risks in an organisation and propose new/modified solutions.	✓	✓	✓	✓	30%	
Examination: 50% (duration: 2 hours)						
AT3. 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%	

** Students must pass BOTH the coursework (AT1-AT2) and the examination (AT3) 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 identify threats and vulnerabilities to information processes and problems related to security; and be able to devise effective technical and managerial solutions.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to identify the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply the concepts and techniques learnt on risk management in simple business scenarios.	High	Significant	Moderate	Basic	Not even reaching marginal levels

AT2. Project	Ability to identify, assess, evaluate, respond to and monitor information systems risk through the use of applicable standards, frameworks and leading practices.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to identify threats and vulnerabilities to information processes; and come up with effective technical and managerial solutions.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to come up with the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply the concepts and techniques learnt on risk management in business situations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT3. Final Examination	Ability to describe the standards, frameworks and leading practices related to identifying, assessing, evaluating, responding to and monitoring information systems risk.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to identify threats and vulnerabilities to information processes and demonstrate an understanding of the related security concepts; and describe how effective technical and managerial solutions can be devised.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to come up with the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to apply the concepts and techniques learnt on risk management in business situations.	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.)

- **Risk Basics**: Threats, vulnerabilities, events, assets, business risk Vs IT risk, enterprise risk management (ERM)
- **Risk Management Basics**: Risk universe, risk appetite, risk map, risk tolerance, risk capacity, risk profile, risk aggregation, risk culture, risk management standards and framework, Risk IT framework
- **Risk Identification**: Risk identification techniques, risk scenarios, risk factors, risk register
- **Risk Assessment and Evaluation**: Qualitative risk analysis, quantitative risk analysis, risk assessment approaches and techniques, assessing and expressing impact, vulnerability assessment
- **Risk Response:** Risk response strategies, information systems controls, control categories, application controls, business continuity planning, incident and change management
- **Risk Monitoring:** Risk communication and reporting, key risk indicators
- **Risk Management for Emerging Technologies:** Such as mobile and wireless, cloud

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.	The Risk IT Framework, Information Systems Audit and Control Association, 2009.
2.	Darril Gibson, Managing Risk in Information Systems, 2nd Edition, 2015 Jones & Bartlett Learning, ISBN: 978-1-284-05595-5.

2.2 Additional Readings

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

1.	CRISC Review Manual 2015, Information Systems Audit and Control Association, Dec 2014, ISBN: 978-1604205909.
2.	CISA Review Manual 2015, Information Systems Audit and Control Association, Nov 2014, ISBN: 978-1604205008.
3.	The Risk IT Practitioner Guide, Information Systems Audit and Control Association, 2009.
4.	Risk Scenarios, Using COBIT 5 for Risk, Information Systems Audit and Control Association, 2014.
5.	Agrawal, Campoe, Pierce, Information Security & IT Risk Management, April 2014, Wiley, ISBN: 978-1-118-33589-5.
6.	Selected readings from the Internet and ISACA.