

# IS4543: RISK MANAGEMENT AND INFORMATION SYSTEMS CONTROL

---

## Effective Term

Semester A 2025/26

## Part I Course Overview

### Course Title

Risk Management and Information Systems Control

### Subject Code

IS - Information Systems

### Course Number

4543

### Academic Unit

Information Systems (IS)

### College/School

College of Business (CB)

### Course Duration

One Semester

### Credit Units

3

### Level

B1, B2, B3, B4 - Bachelor's Degree

### Medium of Instruction

English

### Medium of Assessment

English

### Prerequisites

Nil

### Precursors

Nil

### Equivalent Courses

Nil

### Exclusive Courses

Nil

## Part II Course Details

### Abstract

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).

### Course Intended Learning Outcomes (CILOs)

CILOs		Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify the standards, frameworks and leading practices related to identifying, assessing, evaluating, responding to and monitoring information systems risk.	30	x	x	
2	Describe the nature of threats and vulnerabilities to information processes and related security concepts; and how effective technical and managerial solutions can be devised.	30	x		x
3	Identify the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.	20		x	x
4	Identify the concepts and techniques learnt on risk management in real-life scenarios.	20		x	x

#### 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 gain an understanding of the Risk IT framework, the key concepts of risk governance, risk evaluation, and risk response through examples and cases. Students will practice the techniques in design, implement, monitor and maintain risk-based, efficient and effective information systems controls with in-class discussions and activities.	1, 2, 3	Seminar: 3 hrs/week
2	LTA2. Tutorial	Students will use the following activities 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.	1, 2, 3, 4	Seminar: 3 hrs/week

### Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("- for nil entry)	Allow Use of GenAI?
1	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.	2, 3, 4	20	-	Yes

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

**Continuous Assessment (%)**

50

**Examination (%)**

50

**Examination Duration (Hours)**

2

**Assessment Rubrics (AR)**

**Assessment Task**

AT1. Continuous Assessment

**Criterion**

Ability to identify threats and vulnerabilities to information processes and problems related to security; and be able to devise effective technical and managerial solutions.

**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. Continuous Assessment

**Criterion**

Ability to identify the key activities in deriving risk response options and innovatively apply techniques in assessing, evaluating and effectively monitoring information systems risks.

**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. Continuous Assessment

**Criterion**

Ability to apply the concepts and techniques learnt on risk management in simple business scenarios.

**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. Project

**Criterion**

Ability to identify, assess, evaluate, respond to and monitor information systems risk through the use of applicable standards, frameworks and leading practices.

**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. Project

**Criterion**

Ability to identify threats and vulnerabilities to information processes; and come up with effective technical and managerial solutions.

**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. Project

**Criterion**

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.

**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. Project

**Criterion**

Ability to apply the concepts and techniques learnt on risk management in business situations.

**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. Final Examination

**Criterion**

Ability to describe the standards, frameworks and leading practices related to identifying, assessing, evaluating, responding to and monitoring information systems risk.

**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. Final Examination

**Criterion**

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.

**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. Final Examination

**Criterion**

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.

**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. Final Examination

**Criterion**

Ability to apply the concepts and techniques learnt on risk management in business situations.

**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

## Part III Other Information

**Keyword Syllabus**

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

**Reading List**

**Compulsory Readings**

Title	
1	The Risk IT Framework 2nd Edition, Information Systems Audit and Control Association, ISBN: 978-1604208191
2	Darril Gibson, Managing Risk in Information Systems, 3rd Edition, 2020 Jones & Bartlett Learning, ISBN: 978-1284183719.

**Additional Readings**

<b>Title</b>	
1	CRISC Official Review Manual, 7th Edition Revised, Information Systems Audit and Control Association
2	CISA Official Review Manual, 28th Edition 2024, Information Systems Audit and Control Association
3	The Risk IT Practitioner Guide 2nd Edition, Information Systems Audit and Control Association
4	Risk Scenarios, Using COBIT 5 for Risk, Information Systems Audit and Control Association,
5	Selected readings from the Internet and ISACA.