IS4537: INFORMATION SYSTEMS AUDIT

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Information Systems Audit

Subject Code
IS - Information Systems
Course Number
4537

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
IS4501 Information Systems Audit

Exclusive Courses
Nil

Part II Course Details

Abstract
Information security has become more and more important in today’ s business world. From time to time there are threats and vulnerabilities facing us. This course has been designed to teach us the nature of such threats and vulnerabilities

to information processes so that we can know our enemies and the related technical and managerial solutions for us to counteract with. Besides, through learning the key activities and techniques in performing risk management and information systems control we can know ourselves. To make sure the technical controls and management controls are well designed and functioning properly, role of information systems audit is explained in enhancing asset safeguarding, data integrity, system effectiveness and system efficiency. The other goal of this course is to prepare students in achieving professional qualification as Certified Information Systems Auditor (CISA).

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Demonstrate the knowledge of information systems risk management to assess and manage risks in organizations.	25		x	x
2	Understand the technical nature of information systems threats and the technical and managerial solutions to manage them.	25		x	
3	Evaluate and examine innovative controls relating to business processes and using different control objectives, activities and metrics to monitor and maintenance.	20		x	x
4	Apply appropriate techniques to handle the information systems audit life cycle and the main types of information systems audit.	20		x	x
5	Understand the professional code of ethics of the Information Systems Audit and Control Association.	10	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.

Teaching and Learning Activities (TLAs)

	TLAs	Brief Description	CILO No.	Hours/week (if applicable)
1	TLA1: Lecture	The following items form the content of the lecture:IS audit overview: IS security threats, audit purpose and personnelKey concepts of IS security managementInformation technology risks managementIS audit life cycle and main types of IS auditIS audit concepts and techniques, including Computer Assisted Audit Tools and Techniques (CAATTS)Legal and ethical issues for IT auditors	1, 2, 3, 4, 5	Seminar:3 Hours/Week
2	TLA2: Laboratory	During laboratory sessions, the following activities are used to reinforce the concepts learnt in lectures:Exercises: in form of multiple choice questions, short questions, cases or article readings of the related subjects. There will also be individual exercise on CAATTS.Group Discussion: group discussions in the laboratory aim 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 (e.g. Parameter for GenAI use)
1	AT1: Continuous AssessmentIt consists of attendance and class participation. Each tutorial 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	20	
2	AT2: Mid-Term TestA written mid-term test is developed to assess student's competence level in the middle of the semester.	1, 2	15	
3	AT3: ProjectEach student will participate in group project (about 4 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 provide a 20-minute presentation. This allows students to apply security management concepts and methodology to identify IT risks in an organisation and provide resolutions.	1, 2, 3	15	

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Assessment Rubrics (AR)

Assessment Task

AT1: Continuous Assessment

Criterion

Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.

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 correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.

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
Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.

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
Capability to accurately assess IS audit techniques to IS audit life cycle and main types of IS audit.

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 accurately apply ISACA professional code of ethics and project management techniques.

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:Mid-Term Test

Criterion
Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.

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:Mid-Term Test

Criterion
Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.

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

Criterion
Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.

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

Criterion
Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.

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

Criterion
Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.

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

Criterion
Ability to accurately demonstrate knowledge on risk assessment and risk mitigation.

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

Criterion
Ability to correctly understand the various IS security technical concepts and solutions to mitigate the possible threats facing the organization.

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

Criterion
Capability to critically analyse the main types of audit management, internal control, evidence collection and evaluation techniques for IS audit.

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

Criterion
Capability to accurately assess IS audit techniques to IS audit life cycle and main types of IS audit.

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

Criterion
Ability to accurately apply ISACA professional code of ethics and project management techniques.

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

Information Systems auditing; IT Governance; Information Technology risk management; Information Systems risk control; Information System audit process; Information Systems audit techniques; Information Systems audit life cycle; Legal and ethical issues for Information Technology Auditors.

Reading List

Compulsory Readings

	Title
1	Hunton, J., Bryant, S. and Bagranoff, N., Core Concepts of Information Technology Auditing, Wiley & Sons. ISBN: 0471222933.

Additional Readings

	Title
1	Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 5th edition, Boston, Mass; [London]: Thomson Course Technology, 2011. ISBN: 1285448367.
2	David L. Cannon, CISA: Certified Information Systems Auditor Study Guide, 4th edition, Indianapolis, IN: Wiley Publishing, Inc, 2011. ISBN: 9781119056249.
3	Dhillon, Gurpreet, Principles of Information Systems Security: Texts and Cases, John Wiley, 2007. ISBN: 978-0-471-45056-6.
4	James A. Hall, Tommie Singleton, Information Technology Auditing, 3rd edition, South-Western, Cengage Learning, 2005. ISBN: 1439079110.
5	Weber, Ron, Information Systems Control and Audit, Prentice-Hall, Inc, 1999. ISBN: 0139478701.
6	CISA Review Manual, Information Systems Audit and Control Association, current year.
7	Selected readings from: Computers and Security; ISACA Journal