IS3501: CYBERSECURITY FOR BUSINESS

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Cybersecurity for Business

Subject Code
IS - Information Systems
Course Number
3501

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
Internet is part of our life today and Cybersecurity is becoming extremely important for Internet. This course aims to provide students with an overview of information security knowledge so as to protect an organization’ s information assets.

Upon completion of this course, students are able to make use of privacy and security management models in today’s dynamic business environment. Moreover, students can learn how to apply security knowledge for various business applications.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Describe the concept and key elements in data communication and information security.	25	x	x	
2	Assess the value of information asset and the threats in today’s business environment.	25	x		x
3	Demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.	20		x	x
4	Assess the impacts of the proposed security management solution on the operation of organisations.	15		x	x
5	Exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.	15		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.

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:Security Management Policies & Practices: Identification of information assets and development, documentation, implementation of policies, standards, procedures and guidelines, ethics and legal issues.Basics of Data Communication: Concepts related to fundamentals of data communication and networking, different types of networks and communication services and network management.Security Architecture and Models: Concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment networks, applications and those controls used to enforce various levels of availability, integrity and confidentiality.Access Control Systems and Methodology: Collection of mechanisms that work together to create security architecture to protect assets of the information systems.Cryptography: Principles, means, methods of disguising information to ensure its integrity, confidentiality and authenticity.	1, 2, 3, 4, 5	Seminar: 3 Hours/Week

2	TLA2: Case Studies	Students will be required to work on case studies associated with different aspects of information security management. For each case study, students will carry out analysis and formulate recommendations for appropriate security solutions.	1, 2, 3, 4, 5	Seminar: 3 Hours/Week
3	TLA3: Group Presentation	All students will be required to work in a small group on one of the topics covered in the lecture. They are expected to provide background information, present their critical assessment on particular security problem and make recommendations of how organisation resolve this problem with good security management practices.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	AT1: Tutorial Participation Each tutorial consists of exercises, small group discussions, self-reflection, or student presentations to assess students' understanding of the chosen topics and their abilities to apply their skills.	1, 2, 3, 4, 5	20	
2	AT2: Group Project A group project, which includes a project report and presentation, will be allocated to let students apply security management concepts and methodology to solve security risks in the organisation.	1, 2, 3, 4, 5	30	

Continuous Assessment (%)

50

Examination (%)
50

Examination Duration (Hours)
2

Assessment Rubrics (AR)

Assessment Task
AT1:Tutorial Participation

Criterion
Ability to describe the concept and key elements in data communication and information security.

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:Tutorial Participation

Criterion
Ability to assess the value of information asset and the threats in today’ s business environment.

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:Tutorial Participation

Criterion
Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.

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:Tutorial Participation

Criterion
Capability to assess the impacts of the proposed security management solution on the operation of organisations.

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:Tutorial Participation

Criterion
Ability to exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.

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:Group Project

Criterion
Ability to describe the concept and key elements in data communication and information security.

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:Group Project

Criterion
Ability to assess the value of information asset and the threats in today’ s business environment.

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:Group Project

Criterion
Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.

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:Group Project

Criterion
Capability to assess the impacts of the proposed security management solution on the operation of organisations.

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:Group Project

Criterion
Ability to exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.

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:Examination

Criterion
Ability to describe the concept and key elements in data communication and information security.

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:Examination

Criterion
Ability to assess the value of information asset and the threats in today’ s business environment.

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:Examination

Criterion
Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.

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:Examination

Criterion
Capability to assess the impacts of the proposed security management solution on the operation of organisations.

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:Examination

Criterion

Ability to exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.

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

Privacy and security policies; Security management; Access controls; Data security; Internet security; Ethical and legal issues in cybersecurity.

Reading List

Compulsory Readings

	Title
1	Randall J. Boyle, Raymond R. Panko, Corporate Computer Security, 4/E, 2015, Pearson, ISBN: 978-0-13-354519-7.

Additional Readings

	Title
1	William Stallings, Lawrie Brown, Computer Security, 2/E, Pearson, 2012, ISBN: 978-0-13-277506-9.
2	Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger Davis, Dwayne Williams, Principles of Computer Security, McGraw-Hill Education; 4th edition (December 29, 2015).
3	Michael E. Whitman, Herbert J. Mattord Principles of Informatino Security, Course Technology, 6th edition (March 13, 2017).