CS4394: INFORMATION SECURITY AND MANAGEMENT

Effective Term

Semester A 2022/23

Part I Course Overview

Course Title

Information Security and Management

Subject Code

CS - Computer Science

Course Number

4394

Academic Unit

Computer Science (CS)

College/School

College of Engineering (EG)

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

CS3103 Operating Systems

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

The course provides an overview of the concepts and technologies, management and legal issues for the protection of data during processing, storage and transmission. It is important that information security requirements be understood at the organizational level; appropriate information security policy be derived; cost-effective information security solution be planned and deployed; and evidence to auditors be provided on how well an organization has performed when required.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Describe the major information security technologies and their limitations and applications as countermeasures to IT threats.			x	
2	Describe threats in IT environment; recognize and inquire the relationship of threat, vulnerability, countermeasure, and impact in organizational information security.			x	
3	Describe the information security management framework and formulate basic information security policy for an organization and design appropriate guidelines in implementing the policy by applying appropriate Information Security Management Standards.		x	x	
4	Recognize and critique legal issues in information security.		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	Lecture	Introduce the basic concepts, the relationship of these concepts, and their practical use in information security technology management.	1, 2, 3, 4	3 hours/week

2	Tutorial	Understand concepts related to lectures and discuss some real-life examples in applying the concepts.	1, 2, 3	8 hours/semester
3	Group assignment 1 – simple risk analysis	Students are required to identify threats, vulnerabilities, and countermeasures in a given security scenario, and inquire about their effectiveness.	1	2 hours/week for 4 weeks
4	Group assignment 2 – simple policy statement with solutions	Students are required to design a simple information security policy, recommend controls according to standards, suggest associated guidelines for recommended controls, and suggest some audit questions.	2, 3	2 hours/week for 4 weeks

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Group assignment 1	1	12	
2	Group assignment 2	2, 3	12	
3	Short test	1	6	

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

2

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Assignment 1

Criterion

Ability to identify Threats and Vulnerabilities in Scenarios

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below marginal level

Assessment Task

Assignment 1

Criterion

Ability to understand the relationship among Threats, Vulnerabilities and Countermeasures

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below marginal level

Assessment Task

Assignment 2

Criterion

Ability to write simple but high level information security objectives in a given IT environment with controls proposed based upon a given standard

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)
Below marginal level

Assessment Task
Assignment 2

Criterion
Ability to propose reasonable procedures/guidelines matching the security objectives based upon a given standard

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Below marginal level

Assessment Task
Assignment 2

Criterion
Ability to suggest checklist/questions from the perspective of security auditing matching the security objectives based upon a given standard

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Below marginal level

Assessment Task
Short Test

Criterion

Ability to explain and apply information security technologies as security countermeasures

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below marginal level

Part III Other Information

Keyword Syllabus

Overview of Information Security: Threats, vulnerabilities and countermeasures, organizational requirements. Information Security Technologies: Access Control, Cryptographic techniques, Authentication and Public Key Infrastructures. Information Security Management: Policy, Risk Assessment, and Standards. Legal Issues: Computer Crimes and Forensics, Information Security Audits.

Syllabus

- Overview of Information security
  - Risks and attacks in an information system environment.
  - Requirements on confidentiality, integrity, availability, authentication, non-repudiation
- Information Security Technologies
  - Access control
  - Network security problems, access control methods, firewalls, physical access control, computer access control models, mandatory and discretionary policies, operating system access control
  - Encryption techniques
  - Confidentiality solutions, symmetric encryption, AES, public key encryption, RSA, key management
  - Authentication and Public key Infrastructure
  - Authentication techniques: password, cryptography, biometric; authentication protocols, digital signature, trust models, digital certificates, Certificate Authority, revocation
- Information Security Management
  - Security policies, relationship to business process
  - Security organizations
  - Risk assessment, different approaches
  - Information Security Management Standards
- Legal issues
  - Computer Crimes, disk protection
  - Intellectual property
  - E-commerce law
  - Data protection issues
  - Information Security Audits

Reading List

Compulsory Readings

	Title
1	Whitman and Mattord (2010). Management of Information Security, Cengage Learning, 4th edition.

Additional Readings

	Title
1	Merkow and Breithaupt (2005). Information Security: Principles and Practices. Pearson.
2	Greene (2006). Security Policies and Procedures: Principles and Practices. Pearson.