

CS5292: CYBERSECURITY AUDITS AND COMPLIANCE

Effective Term

Semester A 2026/27

Part I Course Overview

Course Title

Cybersecurity Audits and Compliance

Subject Code

CS - Computer Science

Course Number

5292

Academic Unit

Computer Science (CS)

College/School

College of Computing (CC)

Course Duration

One Semester

Credit Units

3

Level

P5, P6 - Postgraduate 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 provide students with a solid foundation in information systems auditing. Upon completion of the course, students will have gained the knowledge and practical skills needed to understand the theory and practice of information systems audit. They will be able to apply auditing techniques to assess internal controls, evaluate the effectiveness and efficiency of information systems, and manage the audit function for an information system.

Course Intended Learning Outcomes (CILOs)

CILOs		Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Articulate the concepts of general auditing and information systems auditing.	20%	x	x	x
2	Apply the information system auditing methodology and formulate information security policy.	25%	x	x	
3	Evaluate the organization's information technology governance, risk management, information system control and security architecture, business continuity plan, disaster recovery plan, and propose solutions in addressing related issues.	30%	x	x	x
4	Develop knowledge and skills in the application of various types of computer-assisted auditing tools and techniques.	25%	x	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	Lectures and Seminars	Students will learn key concepts and knowledge about information system auditing including auditing process, management, governance, etc. from practitioners' perspective.	1, 2, 3, 4	2 hours/week

2	Tutorials	Students will work on tasks applying selected information system auditing frameworks and techniques, which provide students with hands-on experience in audit and compliance.	1, 2, 3, 4	1 hour/week
---	-----------	---	------------	-------------

Assessment Tasks / Activities (ATs)

ATs		CILO No.	Weighting (%)	Remarks	Allow Use of GenAI?
1	Group Portfolio	1, 2, 3, 4	5	Portfolio including weekly in-class tasks	Yes
2	Quiz	1, 2, 3, 4	25	Individual quiz	No
3	Group Case Study	1, 2, 3, 4	20	A final, larger case study	No

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

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**

Group Portfolio; Group Case Study

Criterion

Ability to apply fundamental concepts and appropriate frameworks in cybersecurity auditing and compliance, and demonstrate the ability to do in-depth analysis and make audit recommendations.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below Marginal

Assessment Task

Quiz

Criterion

Demonstrate knowledge of cybersecurity auditing and compliance, including the ability to analyze specific systems and apply appropriate auditing and compliance frameworks.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below Marginal

Assessment Task

Examination

Criterion

Ability to explain the fundamentals of cybersecurity audits and procedures to ensure compliance and apply relevant techniques in given scenarios.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below Marginal

Part III Other Information

Keyword Syllabus

The syllabus will evolve over time as current topics change, with the goal to cover important public and private enterprise frameworks, and technology-specific issue, such as AI audits, crypto-asset compliance, etc. Further topics can be selected from following. 1) Auditing and internal control: structure and conceptual elements of the audit process, and framework's for internal control. 2) Auditing IT governance control: IT function structuring, computer facility security, disaster recovery planning, and the benefits, risks, and audit issues of IT outsourcing. 3) Auditing operating systems and networks: key threats and risks to operating systems, personal computers, intranet and internet commerce, as well as the control techniques to mitigate them.

Reading List

Additional Readings

Title	
1	Information systems control and audit, Ron Weber, Prentice Hall, 1999, ISBN: 0-13-9478701.
2	Auditor's Guide to IT Auditing (2nd Edition) by Richard E. Cascarino, John Wiley & Sons, 2015.
3	Information Technology Control and Audit (4th Edition) by Sandra Senft, Frederick Gallegos and Aleksandra Davis, CRC Press, 2012.
4	Auditing: A Risk-Based Approach to Conducting a Quality Audit (International Edition) (9th Edition) by Karla M. Johnstone, Audrey A. Gramling and Larry E. Rittenberg, South-Western Cengage Learning, 2014.