Subject Description Form

Subject Code	COMP5578
Subject Title	Cybersecurity Risk Management
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	The objectives of this subject are to: 1. enable the students to understand the fundamentals of cybersecurity and its relationship to risk management. 2. enable the students to understand the fundamentals of risk management as broader scope of technology management. 3. equip the students the ability to apply the disciplines of cybersecurity and risk management onto contemporary industrial applications such as information systems, cyber-physical systems, fintech, artificial intelligence (AI) and machine learning.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: a) acquire a general understanding about the cybersecurity process. b) acquire a general understanding about the risk management process. c) acquire a thorough understanding of cybersecurity and risk management on the protection of data, business continuity, and regulatory compliance. d) understanding various industrial standard on cybersecurity risk management such those from International Organization for Standardization (ISO27001), National Institutional Standards and Technology (Cybersecurity), Information Systems Audit and Control Association (COBIT), Association of Certified Anti-Money Laundering Specialists (CAFCA). e) implement cybersecurity program and projects by identifying business risk / threats / vulnerabilities, establishing mitigation strategies, and delivering appropriate technologies such as artificial intelligence (AI) and machine learning.

	f) adopting other disciplines and methodologies such as quality management, knowledge management, innovation strategies, to enhance the capability and maturity of enterprise cybersecurity.
Subject Synopsis/ Indicative Syllabus	Topic **1. Risk Management for Technology Management** Risk management and risk assessment processes, threats vs vulnerabilities vs controls, residue risks, probability vs business impacts **2. Cybersecurity for Industries** Cybersecurity for information systems, cyber-physical systems, fintech, artificial intelligence (AI) and machine learning; challenge on AI safety and anti-money-laundering (AML) **3. Principles of Information Systems Audit & Control** Implications of information systems / cybersecurity audit, role of auditor, process and methodology, career opportunities **4. Protection of data, business continuity, and regulatory compliance** Principles of data protection for confidentiality, integrity, and availability (CIA), business continuity and resilience, various legal requirements, and regulatory compliances **5. Advanced technology for cybersecurity** Data networking, data / text mining, cloud computing, artificial intelligence, machine learning **6. Contemporary methodologies to enhance the capability and maturity of enterprise cybersecurity** Strategic management, project management, innovation strategy, quality management, and knowledge management.
Teaching/Learning Methodology	This subject emphasises both theoretical and practical aspects of cybersecurity and risk management. It is intended to help students to learn and understand the contemporary discipline of cybersecurity and risk management. Lecture, computer simulations, laboratories, industrial seminars will be combined to provide students with optimal learning experiences.

Assessment Methods in Alignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)					
		a	b	c	d	e	f
1. Continuous Assessment		✓	✓	✓	✓	✓	✓
a. Assignment	10	✓	✓	✓	✓	✓	✓
b. Project	20	✓	✓	✓	✓	✓	✓
c. Tests	25	✓	✓	✓	✓	✓	✓
2. Examination	45	✓	✓	✓	✓	✓	✓
Total	100 %						

- Assignments can be term paper, discussions of contemporary industrial problem and potential solutions. The purpose is to challenge students' understanding on basic theories and industrial trend.
- Tests can be, quizzes, mid-term, to determine the progress of students during the semester.
- Project can be individual-based or group-based, to identify current industrial problems and recommend for actionable projects. This can demonstrate students' capability to handle cybersecurity challenges as related to the subject topics by contemporary technologies and methodologies.

=Student Study Effort Expected

Class contact:	
▪ Class activities (lecture, tutorial, lab, seminar)	39 Hrs.
Other student study effort:	
▪ Assignments, Quizzes, Projects, Exams	66 Hrs.
Total student study effort	105 Hrs.

Reading List and References

1. Cybersecurity : Technology and Governance, Audun Jøsang, Springer Cham. 2025.
2. Developing cybersecurity programs and policies in an AI-driven world Santos, Omar (author), Pearson; 2024; Fourth edition.
3. Cybersecurity Risk Management In Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, Brumfield, Cynthia ; Haugli, Brian Newark: Wiley; 2021; 1st edition
4. ISACA Journals, https://www.isaca.org/resources/isaca-journal
5. Anti-money laundering compliance and the legal profession Kebbell, Sarah (author), Routledge, 2022.
6. Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry, Felix I. Lessambo, Palgrave Macmillan Cham, 2023
7. Understanding AI in Cybersecurity and Secure AI Challenges, Strategies and Trends, Dilli Prasad Sharma, Springer Cham (will publish in July 2025)