UNSW Course Outline

INFS4929 Cybersecurity Leadership and Risk Management - 2024

Published on the 12 May 2024

General Course Information

Course Code : INFS4929
Year : 2024
Term : Term 2
Teaching Period : T2
Is a multi-term course? : No
Faculty : UNSW Business School
Academic Unit : School of Information Systems and Technology Management
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Information systems and information technology (IS/IT) underpin the operation of most facets of most organisations. IS/IT provide means by which organisations process their transactions, the mechanisms by which business stakeholders communicate, the information required to manage

the performance of the business, and the capability for the business to pursue its strategic plans. The reliance on IS/IT by organizations involves a broad range of risks to all the IS/IT assets within and connected to the organizations. These risks relate all standard categories of IS/IT assets including software, hardware, networks, people.

These risks relate to the correct operation of the systems themselves, the integrity and security of the data, information and intellectual property they manage, the development and implementation of new systems and the improvement of existing systems. Poor management of these IS/IT risks can create business risks that have implications for the business's ability to continue its day to day operations, meet its obligations, it reputation and its strategic plans. These IS/IT risks need to be identified and managed in a systematic way.

This course investigates these risks in a systematic manner and looks at the current theory, methods and best practice for their identification, assessment, analysis and mitigation.

Course Aims

The primary goal of this course is to furnish you with fundamental leadership and managerial competencies essential for addressing both emerging and persistent cybersecurity challenges within digital organizations. These challenges encompass the effective governance and risk management of IS/IT assets, spanning software, hardware, networks, and personnel.

Relationship to Other Courses

INFS4929 is jointly taught with INFS5929, which is a core course for MCom specialisation in Cybersecurity.

Course Learning Outcomes

Course Learning Outcomes	Program learning outcomes
CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency planning.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication
CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO7 : Leadership Development
CLO3 : Explain how organisations can best identify, analyse and monitor their IS/IT risks in organisational and team settings.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork
CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication

Course Learning Outcomes	Assessment Item
CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency planning.	• Preparation and Participation • Individual Assignments • Group Assignment • Final Exam
CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.	• Preparation and Participation • Individual Assignments • Group Assignment • Final Exam
CLO3 : Explain how organisations can best identify, analyse and monitor their IS/IT risks in organisational and team settings.	• Preparation and Participation • Individual Assignments • Final Exam
CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.	• Group Assignment • Preparation and Participation • Individual Assignments • Final Exam

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360

Learning and Teaching in this course

Cybersecurity is an essential component of information systems and is of great importance to all businesses as it protects their data and assets from theft and damage. To help students understand the importance of cybersecurity and how an organisation can manage its cybersecurity risk, the learning experience offered by this course will consist of lectures, case discussion, and simulation. A variety of activities are expected: project, homework assignments, and lectures by guest speakers from industry. Homework assignments familiarise the students with the basic concepts and help them develop critical thinking and planning skills. Through the guest lectures, students can learn real world settings in cybersecurity practices. By working on the project, the students conduct researches on modern cybersecurity topics and can better appreciate the efforts required to protect organisations against cybercrime.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Program learning outcomes
Preparation and Participation Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO2 : Problem Solving
Individual Assignments Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork • PLO7 : Leadership Development
Group Assignment Assessment Format: Group	30%	Start Date: 27/06/2024 06:00 PM Due Date: 01/08/2024 06:00 PM	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork
Final Exam Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO7 : Leadership Development

Assessment Details

Preparation and Participation

Assessment Overview

Assessment is based on the student's frequency and quality of contribution to class discussion, and the participation in team activities.

Course Learning Outcomes

- CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency planning.
- CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.
- CLO3 : Explain how organisations can best identify, analyse and monitor their IS/IT risks in organisational and team settings.
- CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.

Detailed Assessment Description

To encourage effective interaction, a mark will be awarded for your participation in terms of your attendance and the degree to which you engage in class discussions. Assessment will be based on your attendance, the frequency and quality of your contribution to class discussion, and your participation in team activities assessed by peer evaluation.

Assessment Length

N/A

Assignment submission Turnitin type

Not Applicable

Individual Assignments

Assessment Overview

Two individual Assignments.

One assignment asks the student to write a risk management plan, and the other assignment is about the reflection after playing a cyberattack simulation.

Course Learning Outcomes

- CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency

planning.
- CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.
- CLO3 : Explain how organisations can best identify, analyse and monitor their IS/IT risks in organisational and team settings.
- CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.

Detailed Assessment Description

There are two individual assignments, each weights 15% of your grade. More details will be announced later.

Assessment Length

TBA

Submission notes

More details will be announced later.

Assessment information

More details will be announced later.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Group Assignment

Assessment Overview

The students are asked to conduct a self-study project on a cybersecurity topic of their interest, complete a written report and make a presentation in Week 10.

Course Learning Outcomes

- CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency planning.
- CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.
- CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.

Detailed Assessment Description

Cybersecurity issues have been evolving rapidly over time, while this course can only cover its fundamental knowledge. Based on their interests, students will be asked to conduct research on a modern cybersecurity topic and complete a written report and a presentation in Week 10.

Topics will be suggested by the instructor. Students are encouraged to conduct literature review and read additional materials to gain knowledge on the topic chosen.

Assessment Length

TBA

Submission notes

The group assignment must be submitted online through Turnitin.

Assessment information

N/A

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Final Exam

Assessment Overview

It will cover materials covered in lectures during Weeks 1 – 10 (inclusive).

Course Learning Outcomes

- CLO1 : Discuss the overall framework of risk management applied to IS security problems, these include risk assessment, risk control, and risk implementation; as well as contingency planning.
- CLO2 : Assess the implications of IS/IT and online environment to security problems in organizations, from a management perspective.
- CLO3 : Explain how organisations can best identify, analyse and monitor their IS/IT risks in organisational and team settings.
- CLO4 : Plan and undertake a preliminary analysis of an organisational IS/IT risks using common IS/IT risk analysis tools and techniques.

Detailed Assessment Description

A final written examination will take place during the University Exam Period

Assessment Length

TBA

Submission notes

TBA

Assessment information

TBA

Assignment submission Turnitin type

Not Applicable

General Assessment Information

Grading Basis

Standard

Requirements to pass course

In order to pass this course, you must achieve a composite mark of at least 50 out of 100.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 27 May - 2 June	Lecture	Topic: Cyber risk management fundamentals
Week 2 : 3 June - 9 June	Lecture	Topic: Identify assets and activities to be protected
Week 3 : 10 June - 16 June	Lecture	Topic: Performing risk assessments
Week 4 : 17 June - 23 June	Lecture	Topic: Determine risk responses
	Assessment	Indiviual assignement 1 (risk management plan) handed out
Week 5 : 24 June - 30 June	Lecture	Topic: Cybersecurity leadership
	Assessment	Group assignment handed out
Week 6 : 1 July - 7 July	Lecture	Flexibility Week (No class)
Week 7 : 8 July - 14 July	Lecture	Topic: Compliance requirements and frameworks
	Assessment	Individual assignment 1 (risk management plan) due
Week 8 : 15 July - 21 July	Lecture	Topic 1: Security incident preparedness Topic 2: Cybersecurity simulation
	Assessment	Individual assignment 2 (simulation reflection) handed out
Week 9 : 22 July - 28 July	Lecture	Topic 1: Cybersecurity simulation debriefing Topic 2: Business continuity planning
	Assessment	Individual assignment 2 (simulation reflection) due
Week 10 : 29 July - 4 August	Presentation	Student project presentation
	Assessment	Group assignment due

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

More details will be provided in the beginning of the term.

Course Resources

Prescribed Resources

The textbook for this course is:

Darril Gibson and Andy Igonor (2022), Managing Risk in Information Systems, 3rd ed., Jones & Bartlett Learning.

Additional readings will be announced in the course.

Recommended Resources

More details will be provided in the beginning of the term.

Additional Costs

N/A

Course Evaluation and Development

We will seek feedback from the students about the offering of this course and use it as a basis for continual improvement. UNSW's myExperience survey is one of the ways in which student evaluative feedback is gathered. In this course, we shall use your course-level feedback, both quantitative and qualitative, to guide our continued review and redesigning of the course.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Chung-Li Tseng		Quad 2087	+61 2 9385 9704	TBA	No	Yes
Lecturer	Aabir Quazi		TBA	TBA	TBA	No	No

Other Useful Information

Academic Information

COURSE POLICIES AND SUPPORT

The Business School expects that you are familiar with the contents of this course outline and the UNSW and Business School learning expectations, rules, policies and support services as listed below:

- Program Learning Outcomes
- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration

- Protocol for Viewing Final Exam Scripts
- Student Learning Support Services

Further information is provided on the key policies and support page.

Students may not circulate or post online any course materials such as handouts, exams, syllabi or similar resources from their courses without the written permission of their instructor.

STUDENT LEARNING OUTCOMES

The Course Learning Outcomes (CLOs) – under the Outcomes tab – are what you should be able to demonstrate by the end of this course, if you participate fully in learning activities and successfully complete the assessment items.

CLOs also contribute to your achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to UNSW graduate capabilities. More information on Coursework PLOs is available on the key policies and support page. For PG Research PLOs, including MPDBS, please refer to the UNSW HDR Learning Outcomes.

Academic Honesty and Plagarism

As a student at UNSW you are expected to display academic integrity in your work and interactions. Where a student breaches the UNSW Student Code with respect to academic integrity, the University may take disciplinary action under the Student Misconduct Procedure. To assure academic integrity, you may be required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Student Code, it is strongly recommended that you complete the Working with Academic Integrity module before submitting your first assessment task. It is a free, online self-paced Moodle module that should take about one hour to complete.

Submission of Assessment Tasks

SPECIAL CONSIDERATION

You can apply for special consideration when illness or other circumstances beyond your control interfere with your performance in a specific assessment task or tasks, including online exams.

Students studying remotely who have exams scheduled between 10pm and 7am local time, are also able to apply for special consideration to sit a supplementary exam at a time outside of these hours.

Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable. To apply, and for further information, see Special Consideration on the UNSW Current Students page.

Special consideration applications will be assessed centrally by the Case Review Team, who will update the online application with the outcome and add any relevant comments. The change to the status of the application immediately sends an email to the student and to the assessor with the outcome of the application.

Please note the following:

1. Applications can only be made through Online Services in myUNSW (see the UNSW Current Students page). Applications will not be accepted by teaching staff. The lecturer-in-charge/ course coordinator will be automatically notified when your application is processed.
2. Applying for special consideration does not automatically mean that you will be granted a supplementary exam or other concession.
3. If you experience illness or misadventure in the lead up to an exam or assessment, you must submit an application for special consideration, either prior to the examination taking place, or prior to the assessment submission deadline, except where illness or misadventure prevent you from doing so.
4. If your circumstances stop you from applying before your exam or assessment due date, you must apply within 3 working days of the assessment or the period covered by your supporting documentation.
5. Under the UNSW Fit To Sit/Submit rule, if you sit the exam/submit an assignment, you are declaring yourself well enough to do so and are cannot subsequently apply for special consideration.
6. If you become unwell on the day of – or during – an exam, you must stop working on your exam, advise your course coordinator or tutor and provide a medical certificate dated within 24 hours of the exam, with your special consideration application. For online exams, you must contact your course coordinator or tutor immediately via email, Moodle or chat and advise them you are unwell and submit screenshots of your conversation along with your medical certificate and application.
7. Special consideration requests do not allow the awarding of additional marks to students.

Further information on Business School policy and procedure can be found under “Special Consideration” on the key policies and support page.

LATE SUBMISSION PENALTIES

For assessments other than examinations, late submission will incur a penalty of 5% per day or part thereof (including weekends) from the due date and time. An assessment will not be accepted after 5 days (120 hours) of the original deadline unless special consideration has been approved. An assignment is considered late if the requested format, such as hard copy or electronic copy, has not been submitted on time or where the 'wrong' assignment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, the LIC may stipulate a different penalty. Details of such late penalties will be available on the course Moodle page.

FEEDBACK ON YOUR ASSESSMENT TASK PERFORMANCE

Feedback on student performance from formative and summative assessment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than a final assessment, will be assessed and students provided with feedback, with or without a provisional result, within 10 working days of submission, under normal circumstances. Feedback on continuous assessment tasks (e.g. laboratory and studio-based, workplace-based, weekly quizzes) will be provided prior to the midpoint of the course.

Faculty-specific Information

PROTOCOL FOR VIEWING FINAL EXAM SCRIPTS

UNSW students have the right to view their final exam scripts, subject to a small number of very specific exemptions. The UNSW Business School has set a protocol under which students may view their final exam script. Individual schools within the Faculty may also set up additional local processes for viewing final exam scripts, so it is important that you check with your School.

If you are completing courses from the following schools, please note the additional school-specific information:

- Students in the **School of Accounting, Auditing & Taxation** who wish to view their final examination script should also refer to this page.
- Students in the **School of Banking & Finance** should also refer to this page.
- Students in the **School of Information Systems & Technology Management** should also refer to this page.

COURSE EVALUATION AND DEVELOPMENT

Feedback is regularly sought from students and continual improvements are made based on this feedback. At the end of this course, you will be asked to complete the myExperience survey, which provides a key source of student evaluative feedback. Your input into this quality enhancement process is extremely valuable in assisting us to meet the needs of our students and provide an effective and enriching learning experience. The results of all surveys are carefully considered and do lead to action towards enhancing educational quality.

QUALITY ASSURANCE

The Business School is actively monitoring student learning and quality of the student experience in all its programs. A random selection of completed assessment tasks may be used for quality assurance, such as to determine the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of Business School programs. All material used for such processes will be treated as confidential.

TEACHING TIMES AND LOCATIONS

Please note that teaching times and locations are subject to change. Students are strongly advised to refer to the Class Timetable website for the most up-to-date teaching times and locations.