UNSW Course Outline

INFS2701 Managing Cybersecurity in the Digital Age - 2024

Published on the 29 Jan 2024

General Course Information

Course Code : INFS2701
Year : 2024
Term : Term 1
Teaching Period : T1
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

With the proliferation of smart devices, interconnected systems and most recently, artificial intelligence, the importance of cybersecurity has never been more critical. Breaches can disrupt lives, businesses, and governments, causing immeasurable harm. Robust cybersecurity systems

are not just necessary; they are critical.

This foundational course introduces essential concepts in organisational cybersecurity management and data governance. Beginning with an exploration of the symbiotic relationship between human and technical influence, we will then build up your understanding of how data governance and cybersecurity management work together. Through independent and teamwork, you will apply your knowledge to real world case studies, and strengthen your problem-solving skills as part of a responsible cybersecurity management practice.

Course Aims

INFS2701 Cyber Security Management and Governance aims to provide a comprehensive journey into cybersecurity management and data governance, equipping students with foundational knowledge on which to build a responsible and skilful career. It does so through an exploration of human and technical influences in cybersecurity, data governance and management frameworks, emphasising ethical and responsible practices. Students will finish the course ready to extend their specialisation experience, and later navigate the ever-evolving landscape of cybersecurity and data governance effectively while upholding ethical standards.

Relationship to Other Courses

The course serves as a core course within the Cybersecurity Management specialisation in the Bachelor of Commerce programme at UNSW. Building upon the foundational knowledge acquired in the prerequisite course, INFS1701 Introduction to Networking and Security, which explores the technical details of cybersecurity, this course takes a managerial perspective in navigating the complex landscape of cybersecurity management. INFS2701 equips students with the essential skills to oversee and strategise cybersecurity initiatives within organisations, emphasising the critical intersection between technology and business operations. By connecting the technical foundation laid in INFS1701 with managerial insights, students are empowered to address contemporary challenges in cybersecurity, positioning them for success in the rapidly evolving digital era.

Course Learning Outcomes

Course Learning Outcomes	Program learning outcomes
CLO1 : Explain the fundamental concepts and processes involved in cybersecurity management.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication
CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.	• PLO1 : Business Knowledge • PLO2 : Problem Solving
CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO5 : Responsible Business Practice
CLO4 : Use regulatory frameworks to assess the legal and ethical implications of cybersecurity practices, including the regulatory impacts on privacy protection and data quality.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO5 : Responsible Business Practice
CLO5 : Collaborate effectively with team members to address cybersecurity challenges, reach consensus on actionable solutions, and communicate findings using language suitable for both technical and non-technical audiences.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork

Course Learning Outcomes	Assessment Item
CLO1 : Explain the fundamental concepts and processes involved in cybersecurity management.	• Individual Report • Group Assignment • Peer Evaluation • Individual Activities
CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.	• Individual Report • Group Assignment • Peer Evaluation • Individual Activities
CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.	• Individual Report • Group Assignment • Peer Evaluation • Individual Activities
CLO4 : Use regulatory frameworks to assess the legal and ethical implications of cybersecurity practices, including the regulatory impacts on privacy protection and data quality.	• Group Assignment • Peer Evaluation • Individual Activities
CLO5 : Collaborate effectively with team members to address cybersecurity challenges, reach consensus on actionable solutions, and communicate findings using language suitable for both technical and non-technical audiences.	• Group Assignment

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360

Learning and Teaching in this course

This course is developed and delivered within the context of the following learning and teaching philosophy.

In addition to students learning the fundamental content of the course, the content is designed to foster critical thinking and to facilitate the acquisition of life-long learning skills. The course and its delivery are designed with a view to assisting the development of problem solving skills. The role of the lecturer/tutor of a course is to facilitate learning. It is recognised that students are individuals who bring a diverse range of experiences, interests and abilities and that these aspects of the student will influence their own learning. The responsibility for learning lies with the student. The role of the lecturer/tutor then, is to provide the environment within which students can participate and contribute, interact and experiment while adding to their own skills and knowledge. An important element of such an environment is that students are encouraged

to engage in cooperative learning in an enjoyable setting, especially in tutorials.

Accordingly, assessment is weighted toward informed, reasoned and well-argued personal opinion based on the contextual factors and constraints presented in the various scenarios and is consequently, not based on the acquisition of knowledge alone.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Program learning outcomes
Individual Report Assessment Format: Individual	25%	Due Date: Week 5: 11 March - 17 March	• PLO1 : Business Knowledge • PLO2 : Problem Solving
Group Assignment Assessment Format: Group	30%	Due Date: Week 10: 15 April - 21 April, Week 11: 22 April - 28 April	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork • PLO5 : Responsible Business Practice
Peer Evaluation Assessment Format: Individual	10%	Due Date: Week 10: 15 April - 21 April	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO4 : Teamwork
Individual Activities Assessment Format: Individual	35%	Due Date: Weekly	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication • PLO5 : Responsible Business Practice

Assessment Details

Individual Report

Assessment Overview

Report on a cybersecurity issue from industry.

Assesses: PLO1, PLO2

BCom students: myBcom course points for PLO2

Course Learning Outcomes

- CLO1 : Explain the fundamental concepts and processes involved in cybersecurity

management.
- CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.
- CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Group Assignment

Assessment Overview

Group presentation and report on a cybersecurity case.

Assesses: PLO1, PLO2, PLO3, PLO4, PLO5

BCom students: myBcom course points for PLO4

Course Learning Outcomes

- CLO1 : Explain the fundamental concepts and processes involved in cybersecurity management.
- CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.
- CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.
- CLO4 : Use regulatory frameworks to assess the legal and ethical implications of cybersecurity practices, including the regulatory impacts on privacy protection and data quality.
- CLO5 : Collaborate effectively with team members to address cybersecurity challenges, reach consensus on actionable solutions, and communicate findings using language suitable for both technical and non-technical audiences.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Peer Evaluation

Assessment Overview

Response to other groups' presentations.

Assesses: PLO1, PLO2, PLO3, PLO4

BCom students: myBcom course points for PLO3

Course Learning Outcomes

- CLO1 : Explain the fundamental concepts and processes involved in cybersecurity management.
- CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.
- CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.
- CLO4 : Use regulatory frameworks to assess the legal and ethical implications of cybersecurity practices, including the regulatory impacts on privacy protection and data quality.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

Individual Activities

Assessment Overview

Weekly activities to build understanding and applied experience.

Assesses: PLO1, PLO2, PLO3, PLO5

BCom students: myBcom course points for PLO5

Course Learning Outcomes

- CLO1 : Explain the fundamental concepts and processes involved in cybersecurity management.
- CLO2 : Assess an organisation's data governance and cybersecurity practices to identify potential risks.
- CLO3 : Examine data governance, data management and cybersecurity practices, and define how they work together to develop an effective cybersecurity solution.
- CLO4 : Use regulatory frameworks to assess the legal and ethical implications of cybersecurity practices, including the regulatory impacts on privacy protection and data quality.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

General Assessment Information

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.

You are expected to complete all assessment tasks for your courses in the School of Information Systems and Technology Management. Classes are highly practical and relevant to your assessments, so you are expected to attend at least 80% of all scheduled classes.

Where group assignments are used, team members are expected to work in a harmonious and professional fashion, which includes adequate management of non-performing members. You should inform your tutor as soon as possible if you experience problems within a project team. You may be required to evaluate the contribution of each team member (including yourself) in group work and marks for individual students may be adjusted based on peer assessment.

Grading Basis

Standard

Requirements to pass course

Achieve an final mark of at least 50 out of 100.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 12 February - 18 February	Lecture	Cybersecurity and data governance imperative: Basic concepts in cybersecurity management
	Tutorial	Cybersecurity and data governance imperative: Basic concepts in cybersecurity management
Week 2 : 19 February - 25 February	Lecture	Introduction to Data Security Risk, Cyberattacks and Incidents
	Tutorial	Introduction to Data Security Risk, Cyberattacks and Incidents
Week 3 : 26 February - 3 March	Lecture	Data Management I (Data Classification and Data Lifecycle Management)
	Tutorial	Data Management I (Data Classification and Data Lifecycle Management)
Week 4 : 4 March - 10 March	Lecture	Data Management II (Data Classification and Data Lifecycle Management)
	Tutorial	Data Management II (Data Classification and Data Lifecycle Management)
Week 5 : 11 March - 17 March	Lecture	Data Governance
	Tutorial	Data Governance
Week 6 : 18 March - 24 March	Other	Flexibility Week
Week 7 : 25 March - 31 March	Lecture	Responsible Practice (Data Quality, Privacy and Compliance)
	Tutorial	Responsible Practice (Data Quality, Privacy and Compliance)
Week 8 : 1 April - 7 April	Lecture	Legal and Ethical Issues in Cybersecurity Management
	Tutorial	Legal and Ethical Issues in Cybersecurity Management
Week 9 : 8 April - 14 April	Lecture	Information Security Policy and Program
	Tutorial	Information Security Policy and Program
Week 10 : 15 April - 21 April	Lecture	Incident Response, Recovery and Review
	Tutorial	Group Project Presentation

Attendance Requirements

Students are strongly encouraged to attend all lectures and review lecture recordings. However, weekly tutorials are conducted face-to-face with in-class activities that are assessed and must be completed by the end of each session.

Course Resources

Prescribed Resources

The main reference textbook is:

Michael Whitman and Herbert Mattord (2018). Management of Information Security, 6th edition, Cengage Learning, Boston, MA, USA.

The textbook (print book and ebook) is available via the University library - https://library.unsw.edu.au

The print book can be purchased at the UNSW Bookshop on campus and online - https://

www.bookshop.unsw.edu.au/

The ebook can be purchased at the UNSW Bookshop digital site - https://unswbookshop.vitalsource.com/

It is not mandatory to purchase the above text. However if you can get your hands on an edition (including older editions), that would be helpful in filling in the gaps in the lecture slides.

Other references will also be provided by the LIC.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Kevin Kuan		Quad 2072	+61 2 9348 1640	By appointment	No	Yes
Lecturer	Maryam Shah bazi		Quad 2070			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.