BUSA3025

Privacy, Cybersecurity, and AI Governance in Organisations

Session 2, In person-scheduled-weekday, North Ryde 2026

Department of Actuarial Studies and Business Analytics

Contents

General Information

Unit convenor and teaching staff
Mauricio Marrone
accg3025@mq.edu.au
See iLearn for consultation hours

Credit points
10

Prerequisites
130cp at 1000 level or above

Corequisites

Co-badged status

Unit description
Cyber security, privacy and responsible application of Artificial Intelligence are three of the biggest issues facing organisations in the digital age. This unit explores how businesses identify and manage these risks as they integrate online systems and artificial intelligence into their operations in Australia and internationally. You'll learn to protect information, navigate privacy laws such as the Australian Privacy Act and GDPR, and address the legal, ethical and governance challenges that arise when new technologies meet real-world business needs. Whether you're passionate about technology, data analysis or business, this unit will give you the knowledge and confidence to tackle tomorrow's digital challenges.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

On successful completion of this unit, you will be able to:

ULO1: Identify and synthesise cybersecurity risks facing modern organisations.

ULO2: Analyse the practical impact of privacy theories on effective business leadership.

ULO3: Apply the principles of responsible Artificial Intelligence in organisational context to build trust.

ULO4: Evaluate privacy risks within business operations by applying Privacy Impact Assessment methodologies.

General Assessment Information

Late Assessment Submission Penalty (written assessments)

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. Submission time for all written assessments is set at 11.55pm. A 1-hour grace period is provided to students who experience a technical concern.

For any late submissions of time-sensitive tasks, such as scheduled tests/exams, performance assessments/presentations, and/or scheduled practical assessments/labs, students need to submit an application for Special Consideration.

Assessment Tasks

Name	Weighting	Hurdle	Due	Groupwork/Individual	Short Extension	AI Approach
Skills development: Persuasive presentation	20%	No	10/11/2026	Individual	No	Observed
Professional practice: Privacy impact assessment report	40%	No	11/08/2026	Individual	Yes	Open
Professional practice: Cybersecurity breach response report	40%	No	Week 7 and Week 8 (as assigned in tutorial)	Individual	No	Observed

Skills development: Persuasive presentation

Assessment Type [1]: Presentation task
Indicative Time on Task [2]: 20 hours
Due: **10/11/2026**
Weighting: **20%**
Groupwork/Individual: Individual
Short extension [3]: No
AI Approach: Observed

The purpose of this assessment is for you to develop your critical analysis and persuasive communication skills by engaging with a contemporary business privacy challenge.

You will research a privacy business problem, develop compelling arguments for your assigned position by creating a 5 minute video presentation of your arguments, and then prepare a rebuttal to an opposing view after being paired with your peer.

Skills in focus:

- Collaboration and communication
- Critical thinking and problem solving
- Global, ethical and environmental citizenship
- Work readiness

Deliverable(s): Video presentation (5 mins) and rebuttal (individual)

Individual assessment

On successful completion you will be able to:

- Analyse the practical impact of privacy theories on effective business leadership.
- Apply the principles of responsible Artificial Intelligence in organisational context to build trust.

Professional practice: Privacy impact assessment report

Assessment Type [1]: Professional task
Indicative Time on Task [2]: 35 hours
Due: **11/08/2026**
Weighting: **40%**
Groupwork/Individual: Individual
Short extension [3]: Yes
AI Approach: Open

The purpose of this assessment is for you to evaluate privacy risks associated with new business initiatives in alignment with relevant regulations and industry best practices.

You will conduct a privacy impact assessment for a proposed business activity, analysing privacy legislation, mapping data flows, identifying vulnerabilities, assessing risks, and recommending mitigation strategies that balance compliance with business goals.

Skills in focus:

- Work readiness
- Critical thinking and problem solving

- Global, ethical, and environmental citizenship
- Discipline knowledge
- Communication skills

Deliverable(s): A professional privacy impact assessment report [2500 words]

Individual assessment

On successful completion you will be able to:

- Identify and synthesise cybersecurity risks facing modern organisations.
- Analyse the practical impact of privacy theories on effective business leadership.
- Apply the principles of responsible Artificial Intelligence in organisational context to build trust.
- Evaluate privacy risks within business operations by applying Privacy Impact Assessment methodologies.

Professional practice: Cybersecurity breach response report

Assessment Type [1]: Presentation task
Indicative Time on Task [2]: 35 hours
Due: **Week 7 and Week 8 (as assigned in tutorial)**
Weighting: **40%**
Groupwork/Individual: Individual
Short extension [3]: No
AI Approach: Observed

The purpose of this assessment is for you to develop your strategic communication and incident response skills by simulating a briefing between a Chief Information Security Officer (CISO) and a Chief Executive Officer (CEO) in the wake of a critical cybersecurity breach.

You will take on the role of the CISO, briefing the CEO on a cybersecurity attack that has impacted the organisation. Your discussion should cover the motives and methods behind the attack, the application of appropriate cybersecurity frameworks to identify and address vulnerabilities, an evaluation of the organisation's incident response against industry best practices, the roles of key business functions in preventing and responding to the breach, and the emerging cybersecurity threats the organisation should prepare for going forward.

To help the CEO (which will be your tutor) prepare for the discussion, you will submit a written briefing report in advance. This report is not assessed but is intended to ensure a productive and informed conversation during the observed discussion.
Skills in focus:

- Communication skills
- Work readiness
- Critical thinking and problem solving
- Discipline knowledge

Deliverable(s): A 5–10 minute observed CISO–CEO discussion conducted during your tutorial session. A written briefing report may be submitted in advance to support the discussion; this report is not assessed.

Individual assessment

On successful completion you will be able to:

- Identify and synthesise cybersecurity risks facing modern organisations.
- Analyse the practical impact of privacy theories on effective business leadership.
- Apply the principles of responsible Artificial Intelligence in organisational context to build trust.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- Academic Success for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation.

[3] An automatic short extension is available for some assessments. Apply through the Service Connect Portal.

Delivery and Resources

Required Text:	Required Texts: As Cyber Security and Privacy are fast-moving topics, a textbook will likely be significantly outdated by the time it reaches print. Consequently, there will be no prescribed textbook.
Unit Web Page:	Available on iLearn
Technology Used and Required:	Students will require access to a computer and the Internet to undertake research and prepare their answers for their assessment tasks. You will need a mobile phone with a camera (or equivalent) to record your debate videos.

Delivery format and other details:	**Lectures:** To make the best use of our face-to-face time, each class will be divided into two parts. The theoretical component will be delivered as pre-recorded online lectures, which you are required to watch before coming to class. Our face-to-face sessions will be dedicated to practical work, where we will apply the concepts covered in the online lectures. Please ensure you have watched the relevant theoretical lecture prior to attending the practical session (see the timetable). The timetable for classes can be found on the University website at: http://timetables.mq.edu.au Students must attend the tutorial in which they are enrolled and may not change tutorials without the prior permission of the course convenor.
Recommended Readings:	There are many cybersecurity and privacy sources of information online. A few worth looking at include: • SecurityAffairs: http://securityaffairs.co/wordpress/ • Krebs on Security: https://krebsonsecurity.com/
Other Course Materials:	Will be made available on iLearn
Workload:	This unit comprises 13 weekly lectures and 12 tutorials (no tutorial in week 1). Many tutorials will require active participation in small group exercises.

Unit Schedule

The schedule below is indicative of the topics we will cover.

Week	Lecture Topic
1	Cyber-security and privacy
2	AI as an Attacker
3	Eyes Everywhere - AI, Surveillance, and Espionage
4	Identifying risks, frameworks and tools
5	Responding to Cyber-security attacks
6	Business roles involvement in minimising cyber-security issues
7	Obligations and safeguarding the digital domain
Break	
8	READING WEEK (NO LECTURE)
9	Privacy in Australia
10	Assessing privacy compliance in businesses
11	Assessing privacy risks in new technologies/businesses
12	Guest Lecturer - Contemporary cyber-security topics
13	Course Review: Engaging with the inherent tensions between cyber-security and privacy

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Assessment Procedure
- Complaints Resolution Procedure for Students and Members of the Public
- Special Consideration Policy

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit connect.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Academic Success

Academic Success provides resources to develop your English language proficiency, academic writing, and communication skills.

- Ask a Study Coach
- Access StudyWISE
- Upload an assignment to Studiosity
- Complete the Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and processes

Student Enquiries

Got a question? Ask us via the Service Connect Portal, or contact Service Connect.

IT Help

For help with University computer systems and technology, visit https://students.mq.edu.au/support/technology/service-desk.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Unit information based on version 2026.03 of the Handbook