ACCG3060

Cyber Security Governance and Ethics

Session 1, In person-scheduled-weekday, North Ryde 2025

Department of Actuarial Studies and Business Analytics

Contents

Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

General Information

Unit convenor and teaching staff
Unit Convenor
Ali Amrollahi
ali.amrollahi@mq.edu.au

Unit Moderator
Mauricio Marrone
mauricio.marrone@mq.edu.au

Credit points
10

Prerequisites
ACCG2050 or PICT2001 or (130cp at 1000 level or above including BUSA2020)

Corequisites

Co-badged status

Unit description
Every person in an organisation is responsible for safe guarding customer data in this era of
increasing cyber threats. This unit is designed for students to gain an understanding of the
regulatory environment, governance (including cyber governance) and ethical issues relating
to cyber security. The objective of the unit is for students to understand the governance and
ethical issues in the constantly evolving cyber security environment created by new digital
technologies.

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: Explain the governance principles and ethical frameworks relevant to cyber
security in a business context.

ULO2: Demonstrate well-reasoned judgement when critically analysing cyber security
governance and ethical challenges.

ULO3: Evaluate how trade-offs between cyber security, cost/resources and business

opportunities/competitive advantage intersect with risk tolerance, good corporate governance, and business ethics.

ULO4: Apply governance principles and ethical frameworks to develop solutions to a variety of governance and ethical challenges relating to cyber security in a range of business contexts.

Assessment Tasks

Name	Weighting	Hurdle	Due
Professional practice: Cyber Security Briefing	40%	No	04/04/2025
Skills development: Cyber challenges	20%	No	02/05/2025
Professional practice: Disrupting your business	40%	No	06/06/2025

Professional practice: Cyber Security Briefing

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **04/04/2025**
Weighting: **40%**

The purpose of this assessment is for you to deliver a Cyber Security briefing to a Senior Executive team.   You will analyse a collection of internal documents to determine long-term security objectives.   Skills in focus: - Digital skills - Communication skills   Deliverable: Written report Individual assessment

On successful completion you will be able to:
- Explain the governance principles and ethical frameworks relevant to cyber security in a business context.
- Demonstrate well-reasoned judgement when critically analysing cyber security governance and ethical challenges.
- Evaluate how trade-offs between cyber security, cost/resources and business opportunities/competitive advantage intersect with risk tolerance, good corporate governance, and business ethics.
- Apply governance principles and ethical frameworks to develop solutions to a variety of governance and ethical challenges relating to cyber security in a range of business contexts.

Skills development: Cyber challenges

Assessment Type [1]: Debate
Indicative Time on Task [2]: 20 hours
Due: **02/05/2025**
Weighting: **20%**

The purpose of this assessment is for you to hone your skills in analyising and evaluating cyber security business challenges. You will debate ethical, financial and legal arguments. Skills in focus: - Critical thinking - Communication skills Deliverable: Video recordings Individual assessment

On successful completion you will be able to:
- Demonstrate well-reasoned judgement when critically analysing cyber security governance and ethical challenges.
- Evaluate how trade-offs between cyber security, cost/resources and business opportunities/competitive advantage intersect with risk tolerance, good corporate governance, and business ethics.
- Apply governance principles and ethical frameworks to develop solutions to a variety of governance and ethical challenges relating to cyber security in a range of business contexts.

Professional practice: Disrupting your business

Assessment Type [1]: Report
Indicative Time on Task [2]: 35 hours
Due: **06/06/2025**
Weighting: **40%**

The purpose of this assessment is for you to gain experience in introducing disruptive technologies into a business. You will critically assess a real-world case study. Skills in focus: - Ethical awareness - Assess disruptive technologies for security Deliverable: Written report Individual assessment

On successful completion you will be able to:
- Explain the governance principles and ethical frameworks relevant to cyber security in a business context.

- Evaluate how trade-offs between cyber security, cost/resources and business opportunities/competitive advantage intersect with risk tolerance, good corporate governance, and business ethics.
- Apply governance principles and ethical frameworks to develop solutions to a variety of governance and ethical challenges relating to cyber security in a range of business contexts.

---

[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
- the Writing Centre 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

Delivery and Resources

Please refer to iLearn

Unit Schedule

Week 1	Introduction
Week 2	Governance Frameworks and Standards (1)
Week 3	Governance Frameworks and Standards (2)
Week 4	Culture and People
Week 5	Information security policy
Week 6	Security program
Week 7	Analysing Cyber Risks
Week 8	Treating Cyber Risks
Week 9	Legal and Compliance
Week 10	Cybersecurity Ethics
Week 11	Security maintenance and technologies

Week 12	Current Issues and future trends in Cybersecurity
Week 13	Review and Conclusion

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.

- Workshops
- Chat with a WriteWISE peer writing leader
- 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 http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

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 2025.03 of the Handbook