



ACCG3060

Cyber Security Governance and Ethics

Session 1, Weekday attendance, North Ryde 2021

Department of Accounting & Corporate Governance

Contents

General Information	2
Learning Outcomes	2
General Assessment Information	3
Assessment Tasks	3
Delivery and Resources	6
Unit Schedule	6
Policies and Procedures	7

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.

Notice

As part of [Phase 3 of our return to campus plan](#), most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to [timetable viewer](#). To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

General Information

Unit convenor and teaching staff

Unit Convenor and Lecturer

Ali Amrollahi

accg3060@mq.edu.au

Moderator

Yvette Blount

accg3060@mq.edu.au

Credit points

10

Prerequisites

ACCG250 or ACCG2050 or PICT201 or PICT2001

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.

General Assessment Information

Late Submission(s): Late assessment must also be submitted through Turnitin. No extensions will be granted. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late (for example, 25 hours late in submission incurs a 20% penalty). Late submissions will not be accepted after solutions have been discussed and/or made available. This penalty does not apply for cases in which an application for [Special Consideration](#) is made and approved. Note: applications for [Special Consideration Policy](#) must be made within 5 (five) business days of the due date and time.

Assessment Tasks

Name	Weighting	Hurdle	Due
Class Participation	10%	No	Each week
Report	40%	No	23:59 Friday of Week 6
Debate	10%	No	23:59 Friday of Week 8
Critical assessment of new technologies	40%	No	23:59 Friday of Week 13

Class Participation

Assessment Type ¹: Participatory task

Indicative Time on Task ²: hours

Due: **Each week**

Weighting: **10%**

Students are expected to actively participate in class discussions and activities. The quality of participation will be assessed by staff using the criteria outlined in the assessment guide.

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.

Report

Assessment Type ¹: Report

Indicative Time on Task ²: 35 hours

Due: **23:59 Friday of Week 6**

Weighting: **40%**

Students will write a report to the Senior Executive team on how contextual elements of a business, including human resources and organisational culture can contribute to an information security program. Students will be given a collection of internal corporate documents which they will have to analyse to determine the long-term security objectives. The students will prepare a written report which they upload to iLearn.

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.

Debate

Assessment Type ¹: Debate

Indicative Time on Task ²: 20 hours

Due: **23:59 Friday of Week 8**

Weighting: **10%**

Students will debate a current cyber security business problem / challenge. Students will prepare a 6-10 minute video of their ethical, financial and legal arguments for- or against- the matter and upload their video to iLearn. Each student will then be randomly allocated to another (opposing) student's video and have 24-hours to prepare a 3-5 minute rebuttal video which they will also

upload to iLearn.

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.

Critical assessment of new technologies

Assessment Type ¹: Report

Indicative Time on Task ²: 35 hours

Due: **23:59 Friday of Week 13**

Weighting: **40%**

Students will apply governance and ethical frameworks to critically assess a proposal to introduce disruptive technologies into a business. The report should cover both information security and ethical aspects of the new technology

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

Required Text:	Whitman, Michael E., and Herbert J. Mattord. <i>Management of information security</i> (6th Edition). Cengage, 2018.
Unit Web Page:	available on iLearn
Technology Used and Required:	<p>Students will require access to a computer and to the Internet so as to undertake research and to prepare their answers for their assessment tasks. You will need a mobile phone with a camera or a GoPro (or equivalent) to record your debate videos.</p> <p>Software: iLearn, VLC Media Player, Microsoft Office, Adobe Acrobat Reader, Internet Browser, Email Client Software, Adobe Premiere Pro can be used to edit videos.</p>
Delivery format and other details:	<p>The timetable for classes can be found on the University website at: http://timetables.mq.edu.au</p> <p>Students must attend all tutorials.</p> <p>Students must attend the tutorial in which they are enrolled and may not change tutorials without the prior permission of the course convenor.</p>
Recommended Readings:	<p>There are many cybersecurity sources of information online. A few worth looking at include:</p> <ul style="list-style-type: none"> • SecurityAffairs: http://securityaffairs.co/wordpress/ • Krebs on Security: https://krebsonsecurity.com/
Other Course Materials:	Will be made available on 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) (<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](#)
- [Grade Appeal Policy](#)
- [Complaint Management 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) (<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) (<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 ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Student Support

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

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to help you improve your marks and take control of your study.

- [Getting help with your assignment](#)
- [Workshops](#)
- [StudyWise](#)
- [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

Students with a disability are encouraged to contact the [Disability Service](#) who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

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 2021.03 of the [Handbook](#)