COMP3320

Cyber Security Management in Practice

Session 2, Online-scheduled-weekday 2026

School of Computing

Contents

General Information

Unit convenor and teaching staff
Lecturer
Michael Chen
michael.chen@mq.edu.au

Convener
Nardine Basta
nardine.basta@mq.edu.au

Credit points
10

Prerequisites
130cp at 1000 level or above and COMP1300 and COMP1350 and COMP2300

Corequisites

Co-badged status

Unit description
This unit provides a practical introduction to cyber security management. It tackles GRC (Governance, Risk Management, Compliance) and incident response. As such, it covers a range of topics including legal and ethical issues, human factor and security culture, legacy systems, security supply chain, regulatory frameworks and policy development, incident triage and business recovery. Effective communication to non-technical audiences plays also a key role in this unit.

Learning in this unit enhances student understanding of global challenges identified by the United Nations Sustainable Development Goals (UNSDGs) Industry, Innovation and Infrastructure

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: Use international frameworks and Standards to develop cyber security policies, standards and procedures as part of an information security management system,

including legal and regulatory compliance.

ULO2: Use qualitative and quantitative risk assessment techniques to both manage cyber security risk by selecting controls and to communicate risk management strategies to business stakeholders.

ULO3: Manage operational security by developing plans to support business continuity and cyber incident response, including digital forensics and evidence management.

General Assessment Information

Module Exam

Assessment Type [1]: Examination Indicative Time on Task [2]: 30 hours Due: **12/10/2026**
Weighting: **30%** Groupwork/Individual: Individual Short extension [3]: No AI Approach: Observed

Students will sit an examination that will test their understanding of the material covered in the unit.

On successful completion you will be able to:

- Use international frameworks and Standards to develop cyber security policies, standards and procedures as part of an information security management system, including legal and regulatory compliance.
- Use qualitative and quantitative risk assessment techniques to both manage cyber security risk by selecting controls and to communicate risk management strategies to business stakeholders.

AI use for Data Breach Analysis

Assessment Type [1]: Portfolio Indicative Time on Task [2]: 40 hours Due: **13/09/2026**
Weighting: **40%** Groupwork/Individual: Individual Short extension [3]: Yes AI Approach: Open

Students will critically evaluate an AI tool's effectiveness in gathering, reporting, and analysing real-world data breaches, with a focus on how well it applies cybersecurity frameworks and risk assessment techniques. They will analyse the tool's outputs to produce a written summary supported by an appendix of source material, demonstrating their ability to assess the reliability and practical value of AI in cybersecurity.

On successful completion you will be able to:

- Use international frameworks and Standards to develop cyber security policies, standards and procedures as part of an information security management system, including legal and regulatory compliance.
- Use qualitative and quantitative risk assessment techniques to both manage cyber security risk by selecting controls and to communicate risk management strategies to business stakeholders.

Junior Analyst Management Update

Assessment Type [1]: Presentation task Indicative Time on Task [2]: 30 hours Due: **08/11/2026**
Weighting: **30%** Groupwork/Individual: Individual Short extension [3]: No AI Approach: Observed

Students will record a video presentation and create a written report that delivers a clear and professional update to management on a cyber incident. The task assesses their ability to communicate effectively with both technical and non-technical audiences using contemporary digital communication and traditional management reporting.

On successful completion you will be able to:

- Manage operational security by developing plans to support business continuity and cyber incident response, including digital forensics and evidence management.

[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.

Assessment Tasks

Name	Weighting	Hurdle	Due	Groupwork/Individual	Short Extension	AI Approach
Module Exam	30%	No	12/10/2026	Individual	No	Observed
AI use for Data Breach Analysis	40%	No	13/09/2026	Individual	Yes	Open
Junior Analyst Management Update	30%	No	08/11/2026	Individual	No	Observed

Module Exam

Assessment Type [1]: Examination
Indicative Time on Task [2]: 30 hours
Due: **12/10/2026**
Weighting: **30%**
Groupwork/Individual: Individual

Short extension [3]: No
AI Approach: Observed

Students will sit an examination that will test their understanding of the material covered in the unit.

On successful completion you will be able to:

- Use international frameworks and Standards to develop cyber security policies, standards and procedures as part of an information security management system, including legal and regulatory compliance.
- Use qualitative and quantitative risk assessment techniques to both manage cyber security risk by selecting controls and to communicate risk management strategies to business stakeholders.

AI use for Data Breach Analysis

Assessment Type [1]: Portfolio
Indicative Time on Task [2]: 40 hours
Due: **13/09/2026**
Weighting: **40%**
Groupwork/Individual: Individual
Short extension [3]: Yes
AI Approach: Open

Students will critically evaluate an AI tool's effectiveness in gathering, reporting, and analysing real-world data breaches, with a focus on how well it applies cybersecurity frameworks and risk assessment techniques. They will analyse the tool's outputs to produce a written summary supported by an appendix of source material, demonstrating their ability to assess the reliability and practical value of AI in cybersecurity.

On successful completion you will be able to:

- Use international frameworks and Standards to develop cyber security policies, standards and procedures as part of an information security management system, including legal and regulatory compliance.
- Use qualitative and quantitative risk assessment techniques to both manage cyber security risk by selecting controls and to communicate risk management strategies to business stakeholders.

Junior Analyst Management Update

Assessment Type [1]: Presentation task
Indicative Time on Task [2]: 30 hours
Due: **08/11/2026**

Weighting: **30%**
Groupwork/Individual: Individual
Short extension [3]: No
AI Approach: Observed

Students will record a video presentation and create a written report that delivers a clear and professional update to management on a cyber incident. The task assesses their ability to communicate effectively with both technical and non-technical audiences using contemporary digital communication and traditional management reporting.

On successful completion you will be able to:

- Manage operational security by developing plans to support business continuity and cyber incident response, including digital forensics and evidence management.

---

[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

Participation in Learning Activities

This unit is online only. Lectures will be streamed live *or* may be pre-recorded and uploaded. The Lectures are not interactive so questions via Zoom may not be answered in real-time. SGTAs are real-time and SGTAs, iLearn, email and phone call are the mechanism to interact with the Lecturer.

ALL Lecture and SGTA material for the whole 13-week unit is available from Week 00 so that students may read ahead and also be prepared, in advance, for active participation in SGTAs. The Assignment is available from Week 00 and students are encouraged to participate in the SGTAs to ask any questions regarding any course material.

The Unit Convenor is also the Lecturer, SGTA presenter and marker for all assessment tasks.

Week 1 classes

This unit is delivered online only. Lectures and SGTA commence in Week 01 and all students are encouraged to participate in the Lectures and SGTA. The Lectures and SGTAs will be later uploaded to iLearn and will be available via Echo360.

Textbooks and Readings

Each lecture will *require* the student to read a provided text selected from a range of cyber security frameworks, Standards, textbooks, guides to best practice, blogs and other sources. Readings will be posted on iLearn and *must* be completed before the tutorial workshop, as the workshops are highly interactive.

A *suggested* (and *highly recommended*) textbook for cyber security studies generally is Smith, Richard E., Elementary Information Security, 3rd ed., Jones & Bartlett Learning, 2020.

Relevant international Standards have been purchased by the University Library and placed in Reserve for use by COMP3320/6325 students.

Lectures

The lecture content of this unit will be delivered online only - please check the timetables page for details. There will be approximately two hours of lecture content each week, which students can view at their own pace if they are unable to view live at the scheduled time.

Small Group Teaching Activities (SGTA)

Students should participate in weekly SGTA online; these activities vary between workshops, practical tasks and tutorials.

Cyber security management is, in large part, about communicating threats and risks to business executives and understanding how to achieve the enterprise's goals while dealing with those threats and risks. Students should therefore expect to develop and make use of their speaking skills during the sessions, and their writing skills during post-workshop discussions on iLearn.

Methods of Communication

We will communicate with you via your university email and through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to the unit convenor via the contact email on iLearn.

Unit Schedule

The unit comprises three modules, with an exam in Week 09 covering the contents of Modules 1 & 2.

Module 1: Governance and Compliance

- Introduction and Overview
- Business and security operations
- Governance, legal and regulatory, frameworks, standards and compliance
- Security architecture, authentication and access control models
- The Human Factor: Policies, culture and communication

Module 2 - Information Risk Management

- Introduction to Information Risk Management
- Threat Intelligence, Qualitative Risk Management
- Estimation, Calibration and Quantitative Risk Management
- Advanced Risk Management

Module 3 - Security Operations

- Business Continuity and Disaster Recovery Planning
- The Incident Response Cycle
- Incident Analysis, logs and SIEM, Security Orchestration and Response
- Digital Forensics and Evidence Management, Crisis Management and Crisis Communications

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.

Changes from Previous Offering

We value student feedback and use it to continually improve the way we offer our units. We encourage students to provide constructive feedback via student surveys, directly to the teaching staff, or through the FSE Student Experience & Feedback link on the iLearn page. Feedback from the previous offering was very positive overall, with students particularly pleased with the level of support from teaching staff. The main exception was the first assessment task, where students raised concerns about its length and complexity. In response, the first assessment has been redesigned, while the rest of the unit's delivery remains unchanged. We will continue to strive to improve both the level of support and student engagement.

Changes since First Published

Date	Description
21/07/2026	Updating assessment due date

Unit information based on version 2026.02 of the Handbook