



COMP8300

Security Management

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

School of Computing

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	2
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	6
<u>Delivery and Resources</u>	8
<u>Unit Schedule</u>	9
<u>Policies and Procedures</u>	9
<u>Changes from Previous Offering</u>	11

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

UC, Lecturer

Milton Baar

milton.baar@mq.edu.au

Contact via 04 1927 9847

Online only

By arrangement

Credit points

10

Prerequisites

COMP6770

Corequisites

Co-badged status

Unit description

The intent of this unit is to provide students with a working knowledge of commercial information security governance requirements, tools and techniques. The unit has a practical focus with workshop and laboratory work that will include aspects of physical security and hacking, information security architectures and the creation of a dummy company on which the tools and techniques will be developed and tested. Topics include an introduction to information security, standard and governance, risk management concepts, security threats, controls, practical hacking, server hardening, evidence collection, business community planning and DRP, creating an enterprise information security framework, and EISF/ISMS certification.

Learning in this unit enhances student understanding of global challenges identified by the United Nations Sustainable Development Goals ([UNSDGs](#)) Industry, Innovation and Infrastructure; Sustainable Cities and Communities; Peace, Justice and Strong Institutions

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: Describe and explain the differences between security frameworks and standards

ULO2: Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk

ULO3: Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment

ULO4: Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

General Assessment Information

Requirements to Pass this Unit

To pass this unit you must achieve a total mark equal to or greater than 50%

Assessment task release dates

ALL assessment tasks details and their due dates are available on iLearn from Week 0.

Automatic short extension

Some assessments are eligible for automatic short extension. You can only apply for an automatic short extension before the due date. If you need more time due to serious issues and for any assessments that are not eligible for Short Extension, you must apply for Special Consideration.

Late Assessment Submission

Late assessments are not accepted in this unit unless a [Special Consideration](#) has been submitted and approved.

Special Consideration

The [Special Consideration Policy](#) aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment.

Written Assessments: If you experience circumstances or events that affect your ability to complete the written assessments in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

Weekly practice-based tasks: To pass the unit you need to demonstrate ongoing development of skills and application of knowledge in all the weekly practical classes. If you miss a weekly practical class due to a serious, unavoidable and significant disruption, contact your convenor ASAP and the other members of your practical group.

Note that a Special Consideration should **only be applied for** if you miss more than two of the weekly practical classes.

Workbook and Document Assessment

Assessment Type ¹: Practice-based task

Indicative Time on Task ²: 20 hours

Due: **2355 30-AUG-2026**

Weighting: **20%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Allowed and encouraged

Students will individually submit workbooks that contain results from group tasks to which they contribute. Submission will comprise a zip file containing images of every page in the workbook than contains writing.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

Document review

Assessment Type ¹: Plan

Indicative Time on Task ²: 30 hours

Due: **2355 20-SEP-2026**

Weighting: **30%**

Groupwork/Individual: Both

Short extension ³: Yes

AI Approach: Allowed and encouraged

Students will individually submit a document detailing their role within a project team, including their specific responsibilities, deliverables, and expected contributions to the final 'Industry Presentation' delivered at the end of the unit. Submission will comprise a zip file containing images of every page in the workbook than contains writing not including the pages submitted for the first assessment task.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

Industry Presentation and Document Review

Assessment Type ¹: Viva/oral examination

Indicative Time on Task ²: 50 hours

Due: **0830 Saturday 7-NOV-2026 in person, location to be confirmed**

Weighting: **50%**

Groupwork/Individual: Both

Short extension ³: No

AI Approach: Not allowed

Students will develop a comprehensive set of ISO27001-compliant cybersecurity management documents covering governance, risk assessment, threat identification, control measures and management responsibilities as the basis for their project. The group will present their findings and recommendations to a panel of Industry Experts. The presentation comprises three components:

1. Submission of the complete created document set, working papers, and all relevant material; this must be emailed to the UC to arrive by 2355 1-NOV-2026.
2. Creation of a 30 minute video, one per group, in which each group member describes their role, what they created, how and why they created it and their contribution to group activity; this must be emailed to the UC to arrive by 2355 1-NOV-2026.
3. On Saturday 7-NOV-2026, **ALL** groups will attend the Industry Presentation that will run from 0830-1300. During that time, each group will have a 30 minute Q&A with the Industry Assessors. **All Group Members of All Groups must remain in the Assessment Room from 0830-1300.**

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements

in a commercial environment

- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

NOTE

The Industry Assessment will focus on what you understand and your ability to accurately and completely describe what you did and why you did it. The production of documents alone is insufficient to pass the Industry Assessment.

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
Workbook and Document Assessment	20%	No	30/08/2026	Individual	No	Observed
Document review	30%	No	20/09/2026	Individual	Yes	Open
Industry Presentation and Document Review	50%	No	07/11/2026	Individual and Group	No	Observed

Workbook and Document Assessment

Assessment Type ¹: Practice-based task

Indicative Time on Task ²: 20 hours

Due: **30/08/2026**

Weighting: **20%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Observed

Students will individually submit workbooks that contain results from group tasks to which they contribute.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

Document review

Assessment Type ¹: Professional task

Indicative Time on Task ²: 30 hours

Due: **20/09/2026**

Weighting: **30%**

Groupwork/Individual: Individual

Short extension ³: Yes

AI Approach: Open

Students will individually submit a document detailing their role within a project team, including their specific responsibilities, deliverables, and expected contributions to the final 'Industry Presentation' delivered at the end of the unit.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

Industry Presentation and Document Review

Assessment Type ¹: Presentation task

Indicative Time on Task ²: 50 hours

Due: **07/11/2026**

Weighting: **50%**

Groupwork/Individual: Individual and Group

Short extension ³: No

AI Approach: Observed

Students will develop a comprehensive cybersecurity risk management document covering governance, risk assessment, threat identification, and control measures as the basis for their project. As a group will present their findings and recommendations to an panel of Industry Experts

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic risk management errors and information exposures; assess various techniques and their suitability as controls

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

This unit is delivered face-to-face, although the lectures are recorded and available on iLearn.

The practical tasks start in Week 01 and builds, week upon week, to a single deliverable assessed on the Saturday of Week 13 by a panel of Industry Experts. The work undertaken on the practical task and its deliverable is usually undertaken by students, sometimes working in groups, off-campus at a time and location that suits them.

Each week, based on the lecture and workshop materials provided, you will gradually build an Information Security Management System (ISMS) that used the ISO/IEC:27001 standards as the framework. In Week 05, the documentation you created to date will be reviewed by the Unit Convenor and, if significant changes are required, you will work with the Unit Convenor to modify what you are doing and how you are doing it. In Week 08, the documentation created to date **as a group** will be reviewed by the Unit Convenor and, if significant changes are required, you will work with the Unit Convenor to modify what you are doing and how you are doing it.

This unit is very heavily front-loaded, that means that the first five weeks require significant individual work to ensure that you are able to produce the documents required for the Week 13

presentation and that you understand what you have produced and why you produced them. The work undertaken from Week 06 is group-assessed and creates fundamental components for the Week 13 presentation. It contributes to your understanding of what you are producing and why you are doing it, and that is the major component of the Industry Assessment.

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 is divided into three modules, Governance (Weeks 01-03), Risk (Weeks 04-08) and Operations (Weeks 09-12).

1. Introduction
2. Standards & Governance
3. ISMS
4. Information Classification
5. Risk Management
6. Qualitative Risk
7. Quantitative Risk
8. Loss Calculations
9. Threats and Controls
10. BCP/DRP
11. Incident Management
12. Forensics
13. Industry Panel preparation

Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central \(https://policies.smq.edu.au\)](https://policies.smq.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 \(https://students.mq.edu.au/support/study/policies\)](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 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 to be able to continually improve the way we offer our units. As such we encourage students to provide constructive feedback via student surveys, to the teaching staff directly, or via the FSE Student Experience & Feedback link in the iLearn page. Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff.

To meet the requirements of the University's introduction of the 3AM assessment framework, all assessment tasks were altered and now comprise a review of individual workbook and documents, a review of group-created documents and a Q&A conducted by an external panel of Industry Experts.

Unit information based on version 2026.03 of the [Handbook](#)