COMP8300

Security Management

Session 2, In person-scheduled-weekday, North Ryde 2022

School of Computing

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 Milton Baar milton.baar@mq.edu.au
Credit points 10
Prerequisites ITEC602 or 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 tutorial 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.

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

Late Assessment Submission

Late assessments are not accepted in this unit unless a Special Consideration has been submitted and approved.

Assessment Tasks

Name	Weighting	Hurdle	Due
Quiz 1	10%	No	Week 5
Mid-semester workbook assessment	40%	No	Week 7
Quiz 2	10%	No	Week 9
Industry Presentation	40%	Yes	Week 13

Quiz 1

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 10 hours
Due: **Week 5**
Weighting: **10%**

A multiple choice quiz covering material from weeks 1-4

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

Mid-semester workbook assessment

Assessment Type [1]: Practice-based task
Indicative Time on Task [2]: 40 hours

Due: **Week 7**
Weighting: **40%**

Review and assessment of the workbook content that contains results from group tasks undertaken from weeks 1-7.

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

Quiz 2

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 10 hours
Due: **Week 9**
Weighting: **10%**

A short-answer quiz covering material from weeks 4-8

On successful completion you will be able to:

- 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

Assessment Type [1]: Viva/oral examination
Indicative Time on Task [2]: 40 hours
Due: **Week 13**

Weighting: **40%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Presentation of completed tasks to an external 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
- 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

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

The practical task starts in Week 2 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, 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 07, the documentation you have created 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 seven weeks require significant group work to ensure that you are able to produce the documents required for the Week 13 presentation.

Unit Schedule

Week/ Date	Lecture Topic
Week 1	**Introduction and Course Outline** • What is information security? • Comparison between perfect security, technical security and commercial security • Discussion of risk, threat, likelihood and other terminology • Hacking, black hat, white hat, grey hat • Introduction of students, background of education/work experience • Course outline and expectations for deliverables
Week 2	**Standards & Governance** • Discussion of different standards and frameworks that they will come into contact with, including ISO27001, ISO27002, Sarbanes-Oxley, PCIDSS, ASIC, COBIT, ITIL • Detailed review of ISO27001 and ISO27002 • Detailed review of SOX and FSRA requirements
Week 3	**Information Risk Management Concepts** • What is risk • How can it be measured • How is it mitigated • What should be protected • Introduction to information assets • The role of an Information Security Officer • How is risk managed in different industries • Can risks be accepted, should a business be risk-averse
Week 4	**Threat Workshop** • What are threats • How are threats measured • Relationship between threats and likelihood • Force Majeure, avoidable threats and how a business reacts to each • Industry specific threats • Technology specific threats • Is privacy a threat?
Week 5	**Controls Workshop** • What are controls • Understanding the relationship between threats, likelihood and controls • Can controls reduce threats
Week 6	**Business Continuity Planning and DRP** • BCP and DRP overview • Why do it • What can go wrong • BCP/DRP development process and linkage with TRA

Week 7	**Creating an Enterprise Information Security Framework** • What is an EISF • How are they assessed (ISO/IEC27001, ITIL, COBIT etc) • Importance of scope and statement of applicability • Plan, Do, Check, Act cycle • Evidence, evidence, evidence • What is an Information Security Management System
Week 8	**Information Classification and Exposures** • What is information classification • How to classify information • Policies and procedures • Perils of over or under classifying information • Information exposures
Week 9	**Practical Hacking** • History of hacking, why hack an environment • What colour hat do you have • Operating systems and application basics • Tools and techniques
Week 10	**Incident Response & Server Hardening** • Definition of hardening • Operating system basics • Network basics • Application basics • Procedures……more procedures……..and more procedures…..
Week 11	**Evidence Collection** • Forensics basics • How to collect • What to collect • Roles and responsibilities • When is it better to leave it alone
Week 12	**Physical Security Reviews**
Week 13	**Industry presentation preparation**

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 ask.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.

Late Assessment Submission

Late assessments are not accepted in this unit unless a Special Consideration has been submitted and approved.

Student Support

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

The Writing Centre

The Writing Centre 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 Enquiries

Got a question? Ask us via AskMQ, 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.

Changes from Previous Offering

The unit has returned to face-to-face teaching so Zoom lectures/workshops are no longer offered.

Industry Presentation on the Saturday of Week 13 is mandatory and face-to-face without the option for Zoom participation.