COMP3320

Cyber Security Management in Practice

Session 1, In person-scheduled-weekday, North Ryde 2022

School of Computing

Contents

General Information

Unit convenor and teaching staff
Convenor/Lecturer/Tutor
Milton Baar
milton.baar@mq.edu.au
Contact via 0419279847
By arrangement using email

Steve Cassidy
steve.cassidy@mq.edu.au

Credit points
10

Prerequisites
(130cp at 1000 level or above and (COMP1300 or COMP107) and (COMP1350 or ISYS114) and (COMP343 or COMP2300))

Corequisites

Co-badged status
COMP6325

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.

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

General Faculty Policy on assessment submission deadlines and late submissions:

Online quizzes, in-class activities, or scheduled tests and exam must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure, students may apply for Special Consideration.

All other assessments must be submitted by 5:00 pm on their due date.

Should these assessments be missed due to illness or misadventure, students should apply for Special Consideration.

Assessments not submitted by the due date will receive a mark of zero **unless** late submissions are specifically allowed as indicated in the unit guide or on iLearn.

Late submissions are **NOT** permitted.

Under no circumstances will submissions will be accepted after solutions have been posted.

Module Examinations

Module Examinations will be scheduled during tutorial timeslots in weeks 5, 9 and 13, and will generally replace that week's tutorial. Your attention is drawn to the university's 'Fit to Sit' policy, which states that by commencing an examination you are certifying yourself as fit to sit that examination. In particular, if you commence a Module Examination late, with insufficient time to finish it, you will *not* be offered a Supplementary Examination. It is the responsibility of students to make sure that they are aware of the time at which the Module Exam will commence.

Supplementary Examinations

Applications for Supplementary Examinations under the Disruption to Studies Policy must be made via AskMQ. If this is approved, the Unit Convenor will *attempt* to schedule an examination at a time convenient to the student and will notify the student of the date and time of the examination in a timely fashion.

Assessment Tasks

Name	Weighting	Hurdle	Due
Weekly lecture and workshop discussion participation	15%	No	Marks accumulate weekly until Week 13

Name	Weighting	Hurdle	Due
Weekly Tasks	10%	No	Each week
Assignment 2	15%	No	Week 13
Module Exam #3	15%	No	Week 13
Assignment 1	15%	No	Week 7
Module Exam #1	15%	No	Week 5
Module Exam #2	15%	No	Week 9

Weekly lecture and workshop discussion participation

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 10 hours
Due: **Marks accumulate weekly until Week 13**
Weighting: **15%**

Participation in weekly discussion (in both lectures and workshops) relating contemporary topics - privacy legislation, security breaches, regulatory changes, etc. - to the methdologies introduced in the lectures and workshops. Discussion will take place in the classroom in the case of on-campus delivery, and for online delivery will be both via Zoom meeting (with participation recorded) and via iLearn discussion forum, so as to not disadvantage students who do not have webcam/microphone or sufficient bandwidth for Zoom, or who prefer written communication.

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

Weekly Tasks

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

Each week material will be followed by a short quiz to test student understanding. The final mark will be calculated from the best 10 of 12 scores achieved by the student.

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

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 8 hours
Due: **Week 13**
Weighting: **15%**

Students are required to present the results of a risk assessment, along with suggested mitigation strategies, in order for a business stakeholder (typically a risk or asset owner) to decide upon the appropriate strategy.

On successful completion you will be able to:

- 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.

Module Exam #3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 6 hours
Due: **Week 13**
Weighting: **15%**

A 50 minutes long written examination worth 20% that will be held in week 13 during practical class. This will test your understanding of material covered in weeks 9 to 12.

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.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 7**
Weighting: **15%**

In this assignment, the student will be required to write a draft issue-specific enterprise security policy, based upon the frameworks and Standards examined in Module 1.

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.

Module Exam #1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 7 hours
Due: **Week 5**
Weighting: **15%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 1 to 4.

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.

Module Exam #2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 7 hours
Due: **Week 9**
Weighting: **15%**

A 50 minutes long written examination worth 20% that will be held in week 9 during practical class. This will test your understanding of material covered in weeks 5 to 8.

On successful completion you will be able to:

- 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.

[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

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 on campus - please check the timetables page for details. Guest lecturers and interview subjects will provide 'real-world' case studies and examples. There will be approximately two hours of lecture content each week, which students can view at their own pace.

Tutorials

Students will be expected to participate in weekly tutorials on campus.

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 tutorial sessions, and their writing skills during post-workshop discussions on iLearn. The importance of engaging in this is reflected in the allocation of 15% of the total assessment to these activities.

Unit Schedule

The unit comprises three major modules, each separately examinable.

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 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.

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

Lectures and tutorials will be on-campus only.