COMP3320

Cyber Security Management in Practice

Session 1, Weekday attendance, North Ryde 2020

Dept of Computing

Contents

General Information

Unit convenor and teaching staff
Convenor and Lecturer
Les Bell
les.bell@mq.edu.au
TBA

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://students.mq.edu.au/important-dates

Learning Outcomes

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.

Assessment Tasks

Name	Weighting	Hurdle	Due
Module Exam #1	20%	No	Week 5
Module Exam #2	20%	No	Week 9
Module Exam #3	20%	No	During examination period
Assignment 1	15%	No	Week 8
Assignment 2	15%	No	Week 13
Weekly Tasks	10%	No	Each week

Module Exam #1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 5**
Weighting: **20%**

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]: 10 hours
Due: **Week 9**
Weighting: **20%**

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.

Module Exam #3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **During examination period**
Weighting: **20%**

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 8**
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.

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.

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.

---

[1] If you need guidance or support to understand or complete this type of assessment, please contact the Learning Skills Team

[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

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

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 lecture, as the lectures are highly interactive workshops.

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

Lectures

The lectures for this unit will be workshop-based, and students are expected to come prepared

for discussion of the issues and challenges posed by the readings. 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 workshop sessions.

In addition, guest lecturers will provide 'real-world' case studies and examples.

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
- 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
- Digital Forensics and Evidence Management

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). 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 *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/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 improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Enquiry Service

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

Equity 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.

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.