COMP6325

Cyber Security Management in Practice

Session 1, Special circumstances 2021

School of Computing

Contents

General Information 2

Learning Outcomes 2

General Assessment Information 3

Assessment Tasks 3

Delivery and Resources 7

Unit Schedule 7

Policies and Procedures 8

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.

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to timetable viewer. To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

General Information

Unit convenor and teaching staff Leslie Bell les.bell@mq.edu.au
Credit points 10
Prerequisites Admission to MInfoTechCyberSec or GradCertInfoTech
Corequisites
Co-badged status COMP3320
Unit description *This unit has an online offering for S2 which is **synchronous**, meaning there will be set times to attend online lectures and tutorials.* 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

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total.

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
Module Examination 2	15%	No	Week 9
Module Examination 3	15%	No	Week 13
Assignment 2	15%	No	Week 13
Weekly discussion participation	15%	No	Weekly
Module Examination 1	15%	No	Week 5
Tutorial Tasks	10%	No	Weekly
Assignment 1	15%	No	Week 7

Module Examination 2

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

Module Examination 2

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 Examination 3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 7 hours
Due: **Week 13**
Weighting: **15%**

Module Examination 3

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 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 13**
Weighting: **15%**

Assignment 2

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 discussion participation

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 10 hours
Due: **Weekly**
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.

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.

Module Examination 1

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

Module Examination 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.

Tutorial Tasks

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

Tutorial Tasks

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 1

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

Assignment 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.

[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 in the form of short videos elaborating on the concepts introduced in the readings. Guest lecturers and interview subjects will provide 'real-world' case studies and examples. There will be approximate two hours of lecture content each week, which students can view at their own pace.

Tutorial Workshops

Students will be expected to participate in weekly tutorial workshops, which will be offered in both on campus (face-to-face) and online (Zoom meeting) format.

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, and/or 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
- Digital Forensics and Evidence Management

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
- Grade Appeal Policy
- Complaint Management 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

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 help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- 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

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

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

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.