COIT12212 *Cyber Security Management*
Term 3 - 2021

Profile information current as at 03/05/2024 01:43 pm

All details in this unit profile for COIT12212 have been officially approved by CQUniversity and represent a learning partnership between the University and you (our student). The information will not be changed unless absolutely necessary and any change will be clearly indicated by an approved correction included in the profile.

General Information

Overview
This unit introduces you to the processes and controls for protecting organisations from cyber security threats. You will learn about management controls such as security governance and policy, risk management, and auditing, as well as processes involving employees and end users that contribute to the protection of an organisation's assets. With recent attacks as case studies, this unit will prepare you to select a range of non-technical measures to minimise future cyber security threats.

Details
Career Level: *Undergraduate*
Unit Level: *Level 2*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites
Pre-requisite: COIT11238 Network Infrastructure Foundations and COIT11223 Information Technology and Society
Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the Assessment Policy and Procedure (Higher Education Coursework).

Offerings For Term 3 - 2021
- Online

Attendance Requirements
All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

Website
This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.

Class and Assessment Overview

Recommended Student Time Commitment

Each 6-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 hours for the unit.

Class Timetable

Regional Campuses
Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

Metropolitan Campuses
Adelaide, Brisbane, Melbourne, Perth, Sydney

Assessment Overview

1. **Written Assessment**
Weighting: 40%
2. **Portfolio**
Weighting: 40%
3. **Presentation**
Weighting: 20%

Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the University's Grades and Results Policy for more details of interim results and final grades.

CQUniversity Policies

All University policies are available on the CQUniversity Policy site.
You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the CQUniversity Policy site.

Previous Student Feedback

Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

Feedback from Student Unit and Teaching Evaluation

Feedback
Students were confused about the word count and asked if tables were included, as several tables are necessary in the final assessment.

Recommendation
The word count guidelines and table contents expectations in assessments will be clarified in the assessments specifications to alleviate students' confusion.

Feedback from Unit Coordinator Self Reflection

Feedback
Students found some of the workshop activities too long.

Recommendation
The relevant workshop activities will be revised

Unit Learning Outcomes

On successful completion of this unit, you will be able to:

1. Discuss the best practice principles, processes and standards in cyber security
2. Compare the role of management, operational and technical controls in delivering cyber security
3. Conduct an organisational cyber security risk analysis
4. Prepare plans for auditing security controls and recovering from security attacks
5. Explain techniques for managing people to ensure secure IT systems.

The Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments and individuals in many countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles. ACS members can use the tool MySFIA to build a skills profile.
This unit contributes to the following workplace skills as defined by SFIA 7 (the SFIA code is included):

- Information Security (SCTY)
- Information Assurance (INAS)

Alignment of Learning Outcomes, Assessment and Graduate Attributes

— N/A Level ◦ Introductory Level • Intermediate Level • Graduate Level ◦ Professional Level ◦ Advanced Level

Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
1 - Written Assessment - 40%	•	•	•	•	•
2 - Portfolio - 40%	•	•	•		

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
3 - Presentation - 20%				•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	5
1 - Communication	•	•	•	•	•
2 - Problem Solving	•	•	•	•	•
3 - Critical Thinking	•	•	•	•	•
4 - Information Literacy	•	•	•	•	•
5 - Team Work			•	•	
6 - Information Technology Competence	•	•	•	•	•
7 - Cross Cultural Competence	•				•
8 - Ethical practice	•	•	•	•	•
9 - Social Innovation					
10 - Aboriginal and Torres Strait Islander Cultures					

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes									
	1	2	3	4	5	6	7	8	9	10
1 - Written Assessment - 40%	•	•	•	•	•	•	•	•		
2 - Portfolio - 40%	•	•	•	•	•	•		•		
3 - Presentation - 20%	•	•	•	•		•	•	•		

Textbooks and Resources

Textbooks

COIT12212

Supplementary

Management of Informatnion Security
Edition: 6th edn (2018)
Authors: Whitman, M
Cengage Learning
Florence , KY , USA
ISBN: 9781337405713
Binding: Paperback

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)

Referencing Style

All submissions for this unit must use the referencing style: Harvard (author-date)
For further information, see the Assessment Tasks.

Teaching Contacts

Mahmoud El Khodr Unit Coordinator
m.elkhodr@cqu.edu.au

Schedule

Week 1 - 08 Nov 2021

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Cybersecurity management	Online resources supplied	None

Week 2 - 15 Nov 2021

Module/Topic	Chapter	Events and Submissions/Topic
Cybersecurity Roles and Responsibilities	Elements of Information Security- Chapter 2	None

Week 3 - 22 Nov 2021

Module/Topic	Chapter	Events and Submissions/Topic
Management of cybersecurity Risk	Management of Information Security- Chapter 6	Weekly Portfolio No submission required

Week 4 - 29 Nov 2021

Module/Topic	Chapter	Events and Submissions/Topic
NIST Cybersecurity Framework	Online resources supplied	Weekly Portfolio No submission required

Vacation Week - 06 Dec 2021

Module/Topic	Chapter	Events and Submissions/Topic

Week 5 - 13 Dec 2021

Module/Topic	Chapter	Events and Submissions/Topic
Cybersecurity policy	Management of Information Security- Chapter 4	Weekly Portfolio No submission required

Week 6 - 20 Dec 2021

Module/Topic	Chapter	Events and Submissions/Topic
Cybersecurity risk mitigation and treatment	Management of Information Security- Chapter 7	**Portfolio Part A** Due: Week 6 Friday (24 December 2021) 11:45 PM AEST Submission via Moodle

Vacation Week - 27 Dec 2021

Module/Topic	Chapter	Events and Submissions/Topic

Week 7 - 03 Jan 2022

Module/Topic	Chapter	Events and Submissions/Topic
In-class presentation	None	Assessment 3 Presentation **Presentation** Due: Week 7 Monday (3 Jan 2022) 8:00 am AEST

Week 8 - 10 Jan 2022

Module/Topic	Chapter	Events and Submissions/Topic
Cybersecurity Contingency Planning	Management of Information Security- Chapter 10	Weekly Portfolio No submission required

Week 9 - 17 Jan 2022

Module/Topic	Chapter	Events and Submissions/Topic
Managing Cybersecurity in Cloud Computing	Online resources supplied	Weekly Portfolio No submission required

Week 10 - 24 Jan 2022

Module/Topic	Chapter	Events and Submissions/Topic
Cybersecurity Technical measures	Online resources supplied	**Portfolio Part B** Due: Week 10 Friday (28 Jan 2022) 11:45 PM AEST Submission via Moodle

Week 11 - 31 Jan 2022

Module/Topic	Chapter	Events and Submissions/Topic
SME cybersecurity guidelines	Online resources supplied	Work on finalising assessment 1

Week 12 - 07 Feb 2022

Module/Topic	Chapter	Events and Submissions/Topic
Ethical challenges for cybersecurity	Online resources supplied	Assessment 1 Report submission deadline **Report** Due: Week 12 Friday (11 Feb 2022) 11:45 pm AEST

Exam Week - 14 Feb 2022

Module/Topic	Chapter	Events and Submissions/Topic
There is no final exam in this unit		None

Term Specific Information

Unit Coordinator Dr Mahmoud Elkhodr:
Email: m.elkhodr@cqu.edu.au; Telephone: (02) 9324 5085; Office: Room 2.09, 400 Kent Street, Sydney Campus.

Assessment Tasks

1 Report

Assessment Type
Written Assessment

Task Description
This assessment can be undertaken in a group of up to 4 students.
You will conduct a comprehensive cybersecurity risk management analysis for a given case study. You are free to either use the risk management framework discussed in the book or the NIST Cybersecurity framework. The output will be a written report.

Assessment Due Date
Week 12 Friday (11 Feb 2022) 11:45 pm AEST
Online via Moodle

Return Date to Students

On certification day

Weighting
40%

Assessment Criteria
You are assessed on your ability to analyse the given scenario and develop a comprehensive cybersecurity risk management report.
The marking criteria include conducting a comprehensive risk analysis, writing a risk mitigation plan and a business continuity plan.
Please refer to the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
Online via Moodle

Learning Outcomes Assessed

- Discuss the best practice principles, processes and standards in cyber security
- Compare the role of management, operational and technical controls in delivering cyber security
- Conduct an organisational cyber security risk analysis
- Prepare plans for auditing security controls and recovering from security attacks
- Explain techniques for managing people to ensure secure IT systems.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Team Work
- Information Technology Competence
- Cross Cultural Competence
- Ethical practice

2 Portfolio

Assessment Type
Portfolio

Task Description
This is an individual assessment. During your weekly workshops, you will conduct cyber security management activities for given case studies, such as developing policies and preparing plans. You must maintain your answers, results and reflections from the workshop activities in an online portfolio. This assessment has two submission parts:

- Part 1- Week of 3,4,5,6 exercises by Friday 11:45 PM AEST of Week 6
- Part 2- Week of 8,9,10 exercises by Friday 11:45 PM AEST of Week 10.

Assessment Due Date

Part 1 due on Friday 11:45 PM of week 6. Part 2 due on Friday 11:45 PM of week 10. Both via Moodle.

Return Date to Students

Within 2 weeks of submission date.

Weighting
40%

Assessment Criteria
All marked workshop exercises will contribute equally to the final 40% mark. Marking for each individual workshop exercise will be based on: Discussion, Relevance, Clarity/effort and frequency. Details of the marking schedule will be available on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Online via Moodle

Learning Outcomes Assessed

- Discuss the best practice principles, processes and standards in cyber security
- Compare the role of management, operational and technical controls in delivering cyber security
- Conduct an organisational cyber security risk analysis

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Team Work
- Information Technology Competence
- Ethical practice

3 Presentation

Assessment Type
Presentation

Task Description
This assessment can be undertaken in a group of up to 4 students.
In this assessment, you are to prepare an Issue Specific Security Policy (ISSP) for a given case study. Your group will be allocated 15 minutes in class to present the ISSP. Distance students will have the option to submit a recording of the presentation in lieu of doing it live in class. Other students may discuss taking this option with the unit coordinator. Details of the marking schedule will be available on the Moodle unit website.

Assessment Due Date
Week 7 Monday (3 Jan 2022) 8:00 am AEST
Presentation in-class or recorded. Submit the slides online by Monday 8:00 AM AEST

Return Date to Students

Within 2 weeks of submission date.

Weighting
20%

Assessment Criteria
In this assessment, you will be judged on your ability to explain the Cybersecurity risks your group have identified and your abilities to develop an ISSP.
You will be marked based on both the quality and accuracy of the ISSP you present, as well as your ability to present the ISSP in a clear and professional manner.
Details of the marking schedule will be available on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
Online via Moodle

Learning Outcomes Assessed

- Prepare plans for auditing security controls and recovering from security attacks
- Explain techniques for managing people to ensure secure IT systems.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence
- Cross Cultural Competence
- Ethical practice

Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the **Student Academic Integrity Policy and Procedure**. This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

What is a breach of academic integrity?
A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

Why is academic integrity important?
A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

Where can I get assistance?
For academic advice and guidance, the Academic Learning Centre (ALC) can support you in becoming confident in completing assessments with integrity and of high standard.

What can you do to act with integrity?

Be Honest
If your assessment task is done by someone else, it would be dishonest of you to claim it as your own

Seek Help
If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)

Produce Original Work
Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem