COIT12212 *Cyber Security Management*
Term 2 - 2021

Profile information current as at 05/05/2024 06:59 am

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 2 - 2021

No offerings for COIT12212

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 SUTE

Feedback
Students found the requirement to find templates and write policies and business plans too onerous.

Recommendation
A basic template will be provided for students.

Feedback from SUTE

Feedback
Students would prefer more consistency in the weekly workshops.

Recommendation
The case study included in assessment 3 will be used for some workshop activities.

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%	●	●	●		
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

Prescribed

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

Additional Textbook Information
Both paper and eBook versions can be purchased at the CQUni Bookshop here: http://bookshop.cqu.edu.au (search on the Unit code).

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

Referencing Style

Information for Referencing Style has not been released yet.
This unit profile has not yet been finalised.

Teaching Contacts

Information for Teaching Contacts has not been released yet.
This unit profile has not yet been finalised.

Assessment Tasks

Information for Assessment Tasks has not been released yet.
This unit profile has not yet been finalised.

Academic Integrity Statement

Information for Academic Integrity Statement has not been released yet.
This unit profile has not yet been finalised.