COIT20265 *Networks and Information Security Project*
Term 2 - 2017

Profile information current as at 03/05/2024 03:44 pm

General Information

Overview

This unit is the capstone for the Networks and Information Security specialisation in the Master of Information Technology course. Students are required to demonstrate the skills that they have developed throughout their studies in this course and apply these skills to an authentic task group project or an industry project. Skills will be demonstrated through the conduct of a group project addressing the production of a research plan, project plan, a quality plan, progress reports and a project report, together with appropriate business analysis and process modelling artefacts such as process improvement models and requirements specifications, and a project report. The project will have a designated customer and students will be required to produce project management artefacts associated with a commercial project. Students will be expected to participate in both regular progress meetings involving relevant stakeholders and in technical meetings. Students are encouraged to include the artefacts produced in the project as part of a work portfolio. Note: If students have undertaken COIT20234 Advanced Network Security Project then this unit cannot be taken.

Details

Career Level: *Postgraduate*
Unit Level: *Level 9*
Credit Points: *12*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.25*

Pre-requisites or Co-requisites

Prerequisites COIT20262 Advanced Network Security COIT20263 Information Security Management COIT20264 Network Design PPMP20007 Project Management Concepts
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 - 2017

- Brisbane
- Distance
- Melbourne
- Rockhampton
- Sydney

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 12-credit Postgraduate unit at CQUniversity requires an overall time commitment of an average of 25 hours of study per week, making a total of 300 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. **Presentation and Written Assessment**
Weighting: 60%
2. **Portfolio**
Weighting: 20%
3. **Group Work**
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 Unit evaluation

Feedback

Students found the project presentations challenging but at the same time extremely valuable to improve their confidence and communication skills.

Recommendation

To provide additional support to the students during their preparation of the project presentations. To make the project presentations a big event and invite academics and the general public to attend.

Unit Learning Outcomes

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

1. Apply the concepts taught in network security specialisation units informed by research and professional best-practice.
2. Assess systems for weaknesses and select and implement appropriate counter measures and controls.
3. Evaluate security protections and assess their level of compliance and effectiveness.
4. Identify “client” or customer requirements and propose solutions.
5. Organise, manage and prioritise tasks in order to address complex real world problems.
6. Select and apply task-appropriate project management and solution development methodologies.
7. Demonstrate productive participation and contribution to a project team or work environment.

Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is in use in over 100 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 at
https://www.acs.org.au/professionalrecognition/mysfia-b2c.html
This unit contributes to the following workplace skills as defined by SFIA. The SFIA code is included:

1. Project Management (PRMG)
2. IT Management (ITMG)
3. Information Security (SCTY)
4. Security Administration (SCAD)
5. IT Governance (GOVN)
6. Technical specialism (TECH)
7. IT Operations (ITOP)
8. Systems Installation/Decommissioning (HSIN)
9. Network Support (NTAS)
10. Network Planning (NTPL)
11. Network Design (NTDS)
12. System Design (DESN).

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	6	7
1 - Presentation and Written Assessment - 60%	•	•	•	•	•	•	•
2 - Portfolio - 20%	•	•	•	•	•	•	•
3 - Group Work - 20%	•	•	•	•	•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes						
	1	2	3	4	5	6	7
1 - Knowledge	○	○	○	○	○	○	○
2 - Communication	○	○	○	○	○	○	○
3 - Cognitive, technical and creative skills	○	○	○	○	○	○	○
4 - Research	○	○	○	○	○	○	○
5 - Self-management	○	○	○	○	○	○	○
6 - Ethical and Professional Responsibility	○	○	○	○	○	○	○
7 - Leadership	○	○	○	○	○	○	○
8 - 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
1 - Presentation and Written Assessment - 60%	○	○	○	○	○	○	○	
2 - Portfolio - 20%	○	○	○	○	○	○	○	
3 - Group Work - 20%	○	○	○	○	○	○	○	

Textbooks and Resources

Textbooks

There are no required textbooks.

Additional Textbook Information
This is a capstone unit and no textbooks are required.

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 styles below:

- American Psychological Association 6th Edition (APA 6th edition)
- Harvard (author-date)

For further information, see the Assessment Tasks.

Teaching Contacts

Edilson Arenas Unit Coordinator
e.arenas@cqu.edu.au

Schedule

Week 1 - 10 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Network Security Project by mentor Form project group	No prescribed textbooks for this unit	Make entries in the Portfolio covering activities performed in this week.

Week 2 - 17 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor Project selection		Make entries in the Portfolio covering activities performed in this week.

Week 3 - 24 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week. Submit Portfolio

Week 4 - 31 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic

Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week. 2. Submit DRAFT network security plan. 3. Submit Project Plan. 4. Submit Group Project Progress Report-1.

Week 5 - 07 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week.

Vacation Week - 14 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 21 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week. Submit Portfolio

Week 7 - 28 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week. 2. Deliver Group Presentation of the implementation of proposed network security plan. 3. Submit Group Project Progress Report-2.

Week 8 - 04 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week.

Week 9 - 11 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week. 2. Submit Portfolio 3. Submit Group Project Progress Report-3.

Week 10 - 18 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week.

Week 11 - 25 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week. 2. Deliver presentation of DRAFT Project Report and Technical Implementation. 3. Submit Group Project Progress Report-4.

Week 12 - 02 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic
Meeting with project mentor		1. Submit FINAL Project Report including Project Working Documents. 2. Submit final portfolio covering activities performed from Week 1 to 12.

Review/Exam Week - 09 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic

Exam Week - 16 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic

Term Specific Information

Dr. Edilson Arenas, PhD.
School of Engineering and Technology, Higher Education Division
CQUniversity Australia, 120 Spencer Street, Melbourne, Victoria, 3000, Australia
Phone +61 03 96160570 | **Email** e.arenas@cqu.edu.au

Assessment Tasks

1 Group Project Report, Ancillary Documentation and Network Security Plan

Assessment Type
Presentation and Written Assessment

Task Description
This is the major assessment for your project and comprises five different parts:

1. DRAFT network security plan (Week 4)
2. Project plan (Week 4)
3. Group presentation on the proposed implementation of Network Security Plan (Week 7)
4. Project report and technical implementation (Week 12)
5. Project Working Documents (Ancillary Documentation) (Week 12)

You are required to work on a project as a group with up to four team members.
Note: Please contact the unit coordinator if you have a genuine problem and are unable to participate in a group.

Assessment Due Date

As per schedule in the Moodle unit website

Return Date to Students

On certification day

Weighting
60%

Assessment Criteria
The project report and technical documentation will be assessed upon the quality of the content. This includes the presentation layout and the depth and breadth of project recommendations adhering to the implementation of a secured computer network. The assessment criteria for each part of the assessment described in the Task Description section is as follows:
Note: Please refer to the unit website in Moodle for submission due dates and detailed marking criteria.
DRAFT network security plan (5%)
Due: Friday, Week 4
You are required to submit a DRAFT network security plan that you believe will mitigate, enhance or address the network security of a chosen organisation (project case study).

Project plan (10%)
Due: Friday, Week 4
You are required to submit a project plan that will include at the minimum the following items: 1) a project charter outlining the project scope, objectives, constraints, statement of work, and project team members; 2) a RACI Matrix showing the roles and responsibilities of each team member; 3) a GANTT chart showing the work breakdown structure (WBS); and, 4) the project risks and proposed mitigation plan.
Group presentation of Network Security Plan(10%)
Due: Friday, Week 7
In this mid-term group presentation you will:

- present the summary of your network security plan that you have produced
- identify and justify your selection of key threats or security challenges to the chosen organisation
- explain what technologies you will implement to mitigate or address such threats and challenges
- describe how you will test the security technologies and the types of policies and/or procedures that you intend to produce

On-campus students: The date and time of this presentation will be determined by your local lecturer/tutor.
Distant students: The time of the presentation and the video conferencing technology employed will be determined on an individual basis.
Project working documents (Ancillary Documentation) **(5%)**
Due: Friday, Week 12
This submission includes the group's important project artefacts/ documents such as outlines of the security plan produced prior to building a project plan, preliminary designs, agendas and minutes of team meetings. This document should be included in the FINAL project report as an Annex with appropriate title page.
Project report and technical implementation (30%)
Due: Friday, Week 12
This assessment is comprised of two different parts:

1. Produce detailed network security plan
2. Identify key security threats or challenges and implement technology to mitigate or address them.

Produce detailed network security plan
The project group is required to produce a detailed security plan for a chosen organisation in order to meet its network security threats and challenges.
Identify key security threats or challenges and implement technology to mitigate or address them
This is a practical activity that requires demonstration of the implementation of your group's network security plan. Your group must identify key threats and challenges, and implement technology to mitigate or address them. The technology has to address key challenges to the organisation's network environment. You should pick an area of network, infrastructure or security that you have already applied in your studies, but you would like to explore in-depth and implement.
Your group needs to show how that was implemented and how the tests were carried. Your group is also required to submit the technical documentation including a test plan, test results and any network security policies and/or procedures that result from your implementation test.

Referencing Style

- American Psychological Association 6th Edition (APA 6th edition)
- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Apply the concepts taught in network security specialisation units informed by research and professional best-practice.
- Assess systems for weaknesses and select and implement appropriate counter measures and controls.
- Evaluate security protections and assess their level of compliance and effectiveness.
- Identify "client" or customer requirements and propose solutions.
- Organise, manage and prioritise tasks in order to address complex real world problems.
- Select and apply task-appropriate project management and solution development methodologies.
- Demonstrate productive participation and contribution to a project team or work environment.

Graduate Attributes

- Knowledge

- Communication
- Cognitive, technical and creative skills
- Research
- Self-management
- Ethical and Professional Responsibility
- Leadership

2 Individual Activity Journal - Electronic Portfolio

Assessment Type
Portfolio

Task Description
This is an individual assessment.
An e-portfolio is a learning tool that enables students to accumulate evidence of learning achievement. In this unit, you will use Mahara as the learning tool.
Please refer to the Moodle unit website for the assessment criteria and detailed instructions on how to create your Mahara portfolio.

Assessment Due Date

Please refer to the unit website in Moodle for more details.

Return Date to Students

Within two weeks of submission

Weighting
20%

Assessment Criteria
The project portfolio is to be maintained by every student individually.
Make entries in your portfolio on each occasion you undertake work on the project, for personal reflections and lessons learned. Essentially, use the portfolio to capture things like:
1) Tasks that you performed
2) Time spent
3) Your contributions to the overall project requirements
4) Challenges faced
5) Reflections
5) Bibliography of researched resource materials such as technical journals, websites, trade magazines, etc.
Entries will be made in the portfolio on a weekly basis at a minimum.
You are required to submit your portfolio entries in weeks 3, 6, 9 and 12 for assessment (4 submissions @ 5 marks each for a total of 20 marks). It is important to maintain this document throughout the term as it is the only component of the unit assessed individually.
Failure to submit a portfolio will disadvantage your overall marks.
The unit website provides further information and specific marking criteria.

Referencing Style

- American Psychological Association 6th Edition (APA 6th edition)
- Harvard (author-date)

Submission
Online

Submission Instructions
Submission Online via Mahara and Moodle using Secret URL. See details in the Moodle site.

Learning Outcomes Assessed

- Apply the concepts taught in network security specialisation units informed by research and professional best-practice.
- Assess systems for weaknesses and select and implement appropriate counter measures and controls.
- Evaluate security protections and assess their level of compliance and effectiveness.
- Identify “client” or customer requirements and propose solutions.
- Organise, manage and prioritise tasks in order to address complex real world problems.
- Select and apply task-appropriate project management and solution development methodologies.
- Demonstrate productive participation and contribution to a project team or work environment.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research
- Self-management
- Ethical and Professional Responsibility
- Leadership

3 Group Progress Reports and Group Presentation of DRAFT Project Report

Assessment Type
Group Work

Task Description
This assessment comprises two different parts:
1. Group progress reports
2. Draft Project Report – Group presentation
Please see complete details in the Moodle Site.

Assessment Due Date

As per Schedule in the Moodle unit Website

Return Date to Students

Within two weeks of submission

Weighting
20%

Assessment Criteria
Progress Reports (4@2% each) - 8%
Each progress report will contain a review of the project. Assessment will be on the completeness of the content of the report.
Presentation - 12%
Each group will be allocated a time in Week 11 to present a *draft* of their project report. Each presentation will be assessed on the following criteria:
Group marks will be based on:
Preparation and consistency of presentation
Set up and use of visual aids
Timing of presentation including Q&A
Continuity and flow from one presenter to the next Presentation content is relevant to the topic
Content is clear, concise and relevant
Response to questions during Q&A
Individual marks for presentation will be based on:
Appropriate dress
Presentation manner
Content is explained well
Please see unit website for more specific marking criteria.

Referencing Style

- American Psychological Association 6th Edition (APA 6th edition)
- Harvard (author-date)

Submission
Online

Submission Instructions
Presentations will have University wide coverage via a video conferencing tool. They might as well be attended by external academics and industry people.

Learning Outcomes Assessed

- Apply the concepts taught in network security specialisation units informed by research and professional best-practice.
- Assess systems for weaknesses and select and implement appropriate counter measures and controls.

- Evaluate security protections and assess their level of compliance and effectiveness.
- Identify “client” or customer requirements and propose solutions.
- Organise, manage and prioritise tasks in order to address complex real world problems.
- Select and apply task-appropriate project management and solution development methodologies.
- Demonstrate productive participation and contribution to a project team or work environment.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research
- Self-management
- Ethical and Professional Responsibility
- Leadership

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