



COIT13236 Cyber Security Project

Term 1 - 2024

Profile information current as at 10/05/2024 12:24 am

All details in this unit profile for COIT13236 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 is the capstone to the Cyber Security specialisation of the Bachelor of Information Technology course. The unit is designed so that you can demonstrate your learning across the whole course of study before making the transition to the next stage of your career. To this end, you are to conduct a group project including the design and implementation of a cyber security plan that meets the client's requirements. Deliverables will include the formal security plan and configured secure infrastructure as part of an overall portfolio of planning and design documentation, scripts, and rules. In order to deliver a robust solution, you will need to choose and employ an appropriate project management methodology. The delivered infrastructure will undergo stress testing and simulated security attack scenarios.

Details

Career Level: *Undergraduate*

Unit Level: *Level 3*

Credit Points: 12

Student Contribution Band: 8

Fraction of Full-Time Student Load: 0.25

Pre-requisites or Co-requisites

Prerequisites: (COIS13064 ICT Project Management or COIT12208 ICT Project Management) and COIT12202 Network Security Concepts
Corequisites: COIT13146 System and Network Administration and (COIT13229 Applied Distributed Systems or COIT13240 Applied Cryptography)

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 1 - 2024

- Brisbane
- Cairns
- Melbourne
- Online
- Rockhampton
- Sydney
- Townsville

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 Undergraduate 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. **Report**

Weighting: 40%

2. **Portfolio**

Weighting: 20%

3. **Written Assessment**

Weighting: 20%

4. **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 Students' informal feedback.

Feedback

Individual contributions should be recognised in group assessments.

Recommendation

Provide clear instruction and marking criteria to recognise individual contributions in the context of group assessments.

Feedback from Students' feedback and teaching team's reflection.

Feedback

Students enjoyed working on real world projects and meeting real clients.

Recommendation

Continue to include real-world projects.

Unit Learning Outcomes

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

1. Analyse cyber security requirements to produce a comprehensive cyber security plan
2. Implement well-documented and tested security technologies to meet a cyber security plan
3. Evaluate security protections for compliance and effectiveness
4. Produce the project management artefacts required in a typical cyber security project
5. Demonstrate productive participation and contribution to a project team or work environment
6. Demonstrate work readiness in terms of technical skills, communication skills, and both professional and ethical behaviour.

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)

- Project Management (PRMG)
- IT Management (ITMG)
- Information Security (SCTY)
- Security Administration (SCAD)
- Enterprise IT Governance (GOVN)
- Specialist Advice (TECH)
- IT Infrastructure (ITOP)
- Systems Installation/Decommissioning (HSIN)
- Network Support (NTAS)
- Network Planning (NTPL)
- Network Design (NTDS)
- Systems Design (DESN)
- Penetration testing (PENT)
- 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	6
1 - Report - 40%	•	•	•			•
2 - Portfolio - 20%				•	•	•
3 - Written Assessment - 20%	•	•	•	•		
4 - Presentation - 20%					•	

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes					
	1	2	3	4	5	6
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						

Textbooks and Resources

Textbooks

There are no required textbooks.

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- Access to computer with webcam, microphone and speakers
- Zoom
- Microsoft Teams
- Portfolium

Referencing Style

All submissions for this unit must use the referencing style: [Harvard \(author-date\)](#)

For further information, see the Assessment Tasks.

Teaching Contacts

Biplob Ray Unit Coordinator

b.ray@cqu.edu.au

Schedule

Week 1 - 04 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with Unit Coordinator (UC)		Meet the entire class to select a topic, create a team, and formulate project specifications. Agree upon a specific meeting time, discuss assessments and reporting requirements for each week.

Week 2 - 11 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor and UC		Introduce yourself to the project mentor and lay out a plan for the term.

Week 3 - 18 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor and UC		

Week 4 - 25 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor and UC		

Week 5 - 01 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
--------------	---------	------------------------------

Weekly meeting with project mentor

Technical Report Due: Week 5 Friday
(5 Apr 2024) 11:59 pm AEST

Vacation Week - 08 Apr 2024

Module/Topic

Chapter

Events and Submissions/Topic

No meeting

Week 6 - 15 Apr 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor
and UC

Week 7 - 22 Apr 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor

**Draft E-portfolio - Project
Webpage** Due: Week 7 Friday (26 Apr
2024) 11:59 am AEST

Week 8 - 29 Apr 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor
and UC

Week 9 - 06 May 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor

Draft Final report Due: Week 9
Friday (10 May 2024) 11:45 pm AEST

Week 10 - 13 May 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor
and UC

Week 11 - 20 May 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor

Week 12 - 27 May 2024

Module/Topic

Chapter

Events and Submissions/Topic

Weekly meeting with project mentor
and UC

Review/Exam Week - 03 Jun 2024

Module/Topic

Chapter

Events and Submissions/Topic

Presentation Day

**Final Report, E-portfolio and
Demonstration/Presentation** Due:
Review/Exam Week Friday (7 June
2024) 11:59 pm AEST

Exam Week - 10 Jun 2024

Module/Topic

Chapter

Events and Submissions/Topic

Term Specific Information

Welcome to Term 1 2024! Have an enjoyable term!
Unit Coordinator - Associate Professor Biplob Ray (b.ray@cqu.edu.au)

Assessment Tasks

1 Technical Report

Assessment Type

Report

Task Description

In this unit, you integrate and apply the knowledge and skills you have gained in your course to an industry-relevant team project. You will undertake a project as a team. Teams should be formed, and the project needs to be decided upon before the end of Week 1, with roles and responsibilities agreed upon at your project meeting in Week 2. Once the project, along with roles and responsibilities, are decided in week 2, a change of topic or team is only allowed in exceptional circumstances with approval from the Unit Coordinator (UC). Further details of the unit are on the Moodle website.

Technical Report Assessment: In this assessment, you will develop a solid plan to execute your selected project. The technical report will show the feasibility and capability of your team to execute the project at the end of the term. An updated version of this report will be part of your final report at the end of the semester. The report must include the following sections at a minimum, but you are welcome to have additional sections as you see fit for the project.

- Detailed description of the project, which will overcome a business problem.
- Identify technical and reporting milestones/deliverables of the project. As different groups are undertaking different projects, you should discuss with your Project Mentor (tutor) the expected deliverables for your project.
- Review existing/competing products, solutions, or literature relevant to the project milestone and include them in the report.
- Specification of requirements, for example, functional, usability, reliability, performance, and security.
- Identify, select, and justify appropriate network and security technologies to solve the problem.
- Design a system model for the project to address the problem. This will be the design of your proposed solution to address the business problem. For example, the design description may detail network/security architectures, logical and/or physical network designs, required protocols, or algorithms involved in the design solution.
- Determine the role and responsibilities of each team member to complete the project. Include capabilities to support the role and responsibilities. Your role must match the available job responsibilities in the seek.com.au web portal.
- A draft budget in a table to show itemised costs and where the fund is coming from.
- Risk assessment and a plan to address those risks. The risk assessment must consider ethical and professional issues relevant to the project.
- List the technical hardware and software components you need to use to implement the proposed solution.

The assessment specification on your Moodle website will further detail the points above.

Format and Submission:

The report should be presented as a formal, technical document (e.g. with title, section headings, references, diagrams, tables). The report must be submitted as a Microsoft Word document. You are encouraged to use the Appendix section of your documents/files for different artefacts. For example, if your group has developed/adopted a risk assessment model to undertake a risk assessment, then the risk assessment model can be included in the appendix. All group documents and technical artefacts must be stored on a Microsoft Teams channel created for your group by the Unit Coordinator and shared with your Project Mentor (tutor) and Unit Coordinator. With prior approval of the Unit Coordinator, a collaborative platform other than Microsoft Teams may be used. While documents are stored in Teams, they must be submitted on Moodle to receive a grade.

You may upload a draft copy of your submissions in your shared Microsoft Team folder two weeks before submission to get feedback from your mentor and UC. The draft will not be graded or mandatory but will help you get feedback for improvements, which may result in a better grade. The assessment specification on your Moodle website will further detail the draft submission in week 3.

Assessment Due Date

Week 5 Friday (5 Apr 2024) 11:59 pm AEST

While documents are stored in Teams, they must be submitted on Moodle to be graded.

Return Date to Students

Week 7 Friday (26 Apr 2024)

Return via Moodle

Weighting

40%

Assessment Criteria

Marking Criteria

Your Report will be marked based on the high-level criteria below. The assessment specification on your Moodle will further unfold the marking criteria below.

1. Problem definition. You should clearly and concisely describe the problem your project is trying to solve.
2. Approach. The methodologies, tools, and techniques you use to solve the problem must be appropriate.
3. Quality and depth. Your proposed project plan and solution design will need to show an investigation into significant depth, and the outputs will need to be of the quality expected of a graduate.
4. Evaluation of ethical and professional issues. Your evaluation must show that you understand the issues and identify the appropriate strategies for handling the problems.
5. Clearly articulates the team's roles, responsibilities, and capabilities.
6. Presentation. For example, formatting, grammar, and referencing.

This unit is 12 credit points and requires significant work every week with frequent assessment deadlines. Catching up will be very hard if you catch up and miss a deadline. Therefore, for all assessments, any late submissions more than seven (7) days after the original deadline will receive 0 marks.

Detailed marking criteria are available on Moodle.

Individual and Group Contributions

On the cover page, you must declare individual contributions (even if you contributed equally) with specific details. If your report does not have an individual contribution declaration, you may receive a deduction as specified in the marking guide in Moodle. The project mentor or Unit Coordinator may seek further information from team members, including via interviews, to evaluate the contributions.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online Group

Submission Instructions

While documents are stored in Teams, they must be submitted on Moodle to be graded. You need to upload only one copy for the entire group in Moodle.

Learning Outcomes Assessed

- Analyse cyber security requirements to produce a comprehensive cyber security plan
- Implement well-documented and tested security technologies to meet a cyber security plan
- Evaluate security protections for compliance and effectiveness
- Demonstrate work readiness in terms of technical skills, communication skills, and both professional and ethical behaviour.

2 Draft E-portfolio - Project Webpage

Assessment Type

Portfolio

Task Description

In this assessment, you will create a public e-portfolio project page, which will include your project details, including all reports and artefacts relevant to your project. The e-portfolio project page will also include weekly individual and group project progress reports. In this assessment,

- you will submit a public e-portfolio link covering and presenting your project details according to your technical reports. You can also include video and another form of presentation to make the project website useful to the public.
- you need to create a project progress reporting section in your e-portfolio project webpage where you will post weekly individual and group progress reports. There is no specific format to report your progress report, but it will be marked based on clarity, illustration (for example, screenshots, video, or other forms), and consistency.

Expectations of Progress Reports: Each progress report must:

- explain your technical progress since the last report (or since the start of the project), with each student referring

- to at least one technical artefact that they have made significant contributions to
- report on the status of tasks completed since the previous progress report and any significant changes with respect to your Project Plan
- list the issues and challenges that have arisen and your approaches to addressing them
- list the priority tasks for the next phase of work (up until the next progress report and/or the end of the project)

You will be expected to answer questions about your progress report during week 9 consultation.

Assessment Due Date

Week 7 Friday (26 Apr 2024) 11:59 am AEST

Online via Moodle

Return Date to Students

Week 9 Friday (10 May 2024)

Two weeks after the due date via Moodle

Weighting

20%

Assessment Criteria

Contribution to Grade

- Quality of the project e-portfolio: 10%
- Individual and Group Progress Report: (5+5) = 10 %

Marking Criteria

Your e-portfolio will be marked based on:

1. Design to ensure the professional and promoting nature of the project e-portfolio site
2. Various media and artefacts like videos to explain your project, easy to find your project progress, plan and link to your project's GitHub page
3. Creativity and clarity of the design and information dissemination, respectively.

Your Project progress report will be marked based on:

1. Genuine and in-depth reflection on your experience of doing the project tasks.
2. Analysis of how this project experience will contribute to your future career goals.
3. Depth and quality of your technical contributions.
4. Ability to plan realistic and significant tasks and to complete planned tasks.
5. Identification of challenges in the project and practical approaches to deal with those challenges.

Failure to publish artefacts on Portfolium will result in 0 marks for the individual and group Project progress reports.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online Group

Submission Instructions

Submit public e-portfolio link and .pdf of your project page via Moodle

Learning Outcomes Assessed

- Produce the project management artefacts required in a typical cyber security project
- Demonstrate productive participation and contribution to a project team or work environment
- Demonstrate work readiness in terms of technical skills, communication skills, and both professional and ethical behaviour.

3 Draft Final report

Assessment Type

Written Assessment

Task Description

In this assessment, you will be able to submit a draft of your final report, which will present finalised form of the technical report submitted in assessment one with additional content about the solution you have come up with. For example, you may update your risk action plan based on your findings during the project, or you may have modified your system model (or solution design) or logical and/or physical network designs based on your new findings while implementing the solution. The draft final report should include all the technical artefacts you have created to address the problem and implement the solution. In addition to your updated technical report content, you must include the

following sections in your final report.

- Variations: what are the variations adapted in the solution since your original plan was submitted in assessment one? and why?
- Was your current skill set enough to perform responsibilities relevant to your role? why or why not?
- Explain the implementation details of your solution. This part must be written as a user manual so anyone can reproduce your work. Feel free to include video, screenshots, and other relevant information helpful to use and implement your solution in a diverse context.
- What difficulties have you encountered, and how did you address them?
- A report of security vulnerability assessment for risk score using DREAD Threat Modelling. You may also perform penetration testing or another form of security evaluation to achieve a DREAD-based risk score.
- Review the report of the e-portfolio of another group.

Assessment Due Date

Week 9 Friday (10 May 2024) 11:45 pm AEST

Online via Moodle

Return Date to Students

Week 11 Friday (24 May 2024)

Two weeks after the due date via Moodle

Weighting

20%

Assessment Criteria

Draft Final Report: 20%

This assessment will be marked based on the following guidelines:

- Content quality and relevance. For example, there should be sufficient technical depth, appropriate contributions presented, interesting and clearly explained content, and reflections on learnings.
- Adhering to specifications detailed in the assessment document
- How well does the report the development since reporting in assessment one?
- Appropriateness of the solution to address the problem statements and project plan laid out in the document.
- Documentation aspect of the project for reproducing/implementing the solution by another team
- Quality and completeness of risk scoring for the proposed solution.
- Quality of the review report.

The assessment specification on your Moodle website will further detail each of the points above.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online Group

Submission Instructions

Submit public e-portfolio link and .pdf of your project page via Moodle

Learning Outcomes Assessed

- Analyse cyber security requirements to produce a comprehensive cyber security plan
- Implement well-documented and tested security technologies to meet a cyber security plan
- Evaluate security protections for compliance and effectiveness
- Produce the project management artefacts required in a typical cyber security project

4 Final Report, E-portfolio and Demonstration/Presentation

Assessment Type

Presentation

Task Description

In this final assessment, you will submit the final version of the e-portfolio and report accompanying a demonstration and presentation in front of public audiences. Please submit the following material below via Moodle.

- Final and complete version of the e-portfolio: 5%.
- Final report that addressed feedback and comments on your draft report: 5%.
- Upload PowerPoint slides and perform demonstrative presentation: (5+5) =10%.

Updated Version of e-portfolio:

- Should report 12 weekly individual and group progress reports.
- Presented the project and state of artefacts to date upon completion.
- Clarity and professional presentation.

Final report:

- Need to address all feedback and comments from mentor and/or supervisor.
- Update the rest of the content if required based on the development of the project's solution implementation.

Upload PowerPoint and perform demonstrative presentation:

- Upload PowerPoint slides or any other materials like video demonstration.
- Present your project and demonstrate the solution live as per schedule.

You may receive a Zero (0) in this assessment If you fail to appear on the planned demonstration/presentation day. The assessment specification on your Moodle website will further detail each of the points above.

Assessment Due Date

Review/Exam Week Friday (7 June 2024) 11:59 pm AEST

The demonstrative presentation will be @week 13. See the schedule on Moodle website for the specific due date of your demonstrative presentation.

Return Date to Students

Certification of Grades

Weighting

20%

Assessment Criteria

The e-portfolio will marked based on the criteria below.

- Completeness and clarity.
- Up to date content.
- Various artefacts and media will be used to make the project website useful to the general public.

Marking Criteria of Final Report:

- Does the report adhere to a formal reporting style, like a table of contents, labeling figures, and so on?
- Did the final report address all feedback and suggestions satisfactorily?

Marking Criteria of Final Presentation: It is a group presentation where all group members must present. All members will receive the same group score (unless there are exceptional circumstances, e.g., one member does not give). The score will be based on how you give your part and answer questions. Different students in your team may receive different individual scores. The presentation will be marked based on the following.

- Demonstration of prototype/system [Group]. For example, appropriate technologies are chosen and shown, demonstrating the application of knowledge and skills.
- Presentation organization and flow [Group]. For example, keeping to time limit, preparedness, visual aids, and quality of demonstrations.
- Presentation skills [Individual]. For example, speaking skills, confidence, responding to questions, and demonstrating understanding of the content.

The assessment specification on your Moodle website will further detail each of the points above.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online Group

Submission Instructions

Reports and presentation slides - online via Moodle | Demonstrative presentation - as per given schedule on Moodle website.

Learning Outcomes Assessed

- Demonstrate productive participation and contribution to a project team or work environment

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