



COIT12202 Network Security Concepts

Term 2 - 2022

Profile information current as at 14/12/2025 12:43 pm

All details in this unit profile for COIT12202 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

As the Internet becomes more pervasive, so do the threats to the security of our computer systems and communications. This unit provides you with grounding in security technology. You will study common network security attacks, then the technologies to defend against those attacks. These technologies include cryptography, access control, authentication, firewalls, and wireless network protocols. This unit provides security knowledge that is required for industry standard certification exams, such as CompTIA.

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

Prerequisite: COIT12206 OR COIT13147

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 - 2022

- 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 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: 25%

2. **Online Quiz(zes)**

Weighting: 30%

3. **Written Assessment**

Weighting: 45%

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 Feedback

Feedback

The students are satisfied with the unit materials and the assessment tasks.

Recommendation

Continue maintaining the provided learning and teaching materials and follow the same assessment structure.

Feedback from Staff Feedback

Feedback

This unit could include some topics such as security for cloud computing and IoT applications to meet the industry needs.

Recommendation

Include content related to security for cloud computing and IoT applications in this unit.

Unit Learning Outcomes

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

1. Describe key security concepts and principles
2. Discuss how common security attacks and defences work
3. Explain the role of cryptographic mechanisms in providing computer and network security
4. Apply access control technologies, including firewalls and authentication, to secure computer networks
5. Explain threats and defences that are specific to wireless networks.

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:

- Information Security (SCTY)
- Penetration Testing (PENT)
- Network Support (NTAS)
- Security Administration (SCAD)
- Problem Management (PBMG)
- Data Analysis (DTAN)
- System Design (DESN)
- Incident Management (USUP)

Alignment of Learning Outcomes, Assessment and Graduate Attributes



Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
1 - Written Assessment - 25%	•	•	•		
2 - Written Assessment - 45%				•	•
3 - Online Quiz(zes) - 30%	•	•	•	•	•

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 - 25%	•	•	•	•		•				
2 - Written Assessment - 45%	•	•	•	•		•		•		
3 - Online Quiz(zes) - 30%	•	•	•			•				

Textbooks and Resources

Textbooks

COIT12202

Prescribed

CompTIA security+ guide to network security fundamentals

Edition: 6th (2017)

Authors: Ciampa, M

Cengage

Boston , Massachusetts , USA

ISBN: 978-1-337-28878-1

Binding: Paperback

Additional Textbook Information

Both paper and eBook copies can now 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:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- VirtualBox - A Virtualization Software Package
- Wireshark - Network Protocol Analyser

Referencing Style

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

For further information, see the Assessment Tasks.

Teaching Contacts

Yufeng Lin Unit Coordinator

y.lin@cqu.edu.au

Schedule

Week 01 - 11 Jul 2022

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Security	Chapter 1	

Week 02 - 18 Jul 2022

Module/Topic	Chapter	Events and Submissions/Topic
Threats	Chapter 2 & 5	

Week 03 - 25 Jul 2022

Module/Topic	Chapter	Events and Submissions/Topic
Hash Algorithms and Symmetric Cryptographic Algorithms	Chapter 3	

Week 04 - 01 Aug 2022

Module/Topic	Chapter	Events and Submissions/Topic
Asymmetric Cryptographic Algorithms (Digital Signature and Certificate)	Chapter 3 & 4	
Week 05 - 08 Aug 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Public Key Infrastructure and Cryptographic Transport Protocols	Chapter 4	Quiz 1 Due: Week 5 Friday (13 Aug 2021) 11:45 pm AEST
Vacation Week - 15 Aug 2022		
Module/Topic	Chapter	Events and Submissions/Topic
- MID-TERM BREAK -		
Week 06 - 22 Aug 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Network Security Devices, Design, and Technology	Chapter 6	SHORT-ANSWER QUESTIONS Due: Week 6 Friday (26 Aug 2022) 11:45 pm AEST
Week 07 - 29 Aug 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Administering a Secure Network	Chapter 7	
Week 08 - 05 Sep 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Access Management	Chapter 12	
Week 09 - 12 Sep 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Identity Management	Chapter 11	
Week 10 - 19 Sep 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Wireless Network Security	Chapter 8	
Week 11 - 26 Sep 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Mobile and Embedded Device Security	Chapter 10	Quiz 2 Due: Week 11 Friday (1 Oct 2021) 11:45 pm AEST
Week 12 - 03 Oct 2022		
Module/Topic	Chapter	Events and Submissions/Topic
Summary of the Unit.		
Review/Exam Week - 10 Oct 2022		
Module/Topic	Chapter	Events and Submissions/Topic
No exam for COIT12202.		REPORT Due: Review/Exam Week Monday (10 Oct 2022) 11:45 pm AEST
Exam Week - 17 Oct 2022		
Module/Topic	Chapter	Events and Submissions/Topic
No exam for COIT12202.		

Term Specific Information

Some tutorial practices need administrator privileges, and you may be required to complete those tasks on your own computer. If you are concerned about installing any of the needed software on your computer, you can create virtual machines (Windows/Linux) for the lab practices. The needed software installed in the virtual machines will not impact the host computer.

Assessment Tasks

1 SHORT-ANSWER QUESTIONS

Assessment Type

Written Assessment

Task Description

This assessment (Short-Answer Questions) is designed to test students' understanding of information security including the basic concepts of information security, threats, cryptography, public key infrastructure, and cryptographic transport protocols. The assessment task contains a series of short-answer questions related to the contents in weeks 1-5. Further details, including what you are required to submit, will be available on the Moodle unit website.

Assessment Due Date

Week 6 Friday (26 Aug 2022) 11:45 pm AEST

Return Date to Students

Week 8 Friday (9 Sept 2022)

Assessments will be returned through Moodle. Late submissions with or without extension approvals may be returned after the above date.

Weighting

25%

Assessment Criteria

For short-answer questions, the answers will be assessed in regard to accuracy, clarity, and details.

Detailed marking criteria will be provided on Moodle. Assignments received 14 days or more after the due date will not be marked and will receive zero.

Referencing Style

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

Submission

Online

Submission Instructions

Submission instructions are provided in Moodle.

Learning Outcomes Assessed

- Describe key security concepts and principles
- Discuss how common security attacks and defences work
- Explain the role of cryptographic mechanisms in providing computer and network security

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence

2 ONLINE QUIZ(ZES)

Assessment Type

Online Quiz(zes)

Task Description

There will be two online quizzes (Quiz 1 and Quiz 2).

The quizzes will consist of a series of True/False, Multiple Choice, and Analytical questions. Questions will be randomly selected from a pool of questions on topics from weeks 1 to 4 for Quiz 1 and from weeks 5 to 10 for Quiz 2.

You are unlikely to be asked the same questions as other students, nor the same questions in subsequent attempts at the quiz.

The time limit for each attempt is 1 hour. The quiz automatically closes - if you have not submitted an attempt at the quiz by the due date, you will receive zero.

You are allowed to attempt the quizzes multiple times and the result of your last submission will be your final marks of the quiz. Details will be provided on the Moodle unit website.

Number of Quizzes

2

Frequency of Quizzes**Assessment Due Date**

Quiz 1 is due on Friday in week 5 (12 August) and Quiz 2 is due on Friday in week 11 (30 September). See Moodle website for more details.

Return Date to Students

Quiz marks and answers will be released immediately after the deadline of each quiz.

Weighting

30%

Assessment Criteria

The quizzes are automatically graded by the system based on the selection of correct or incorrect answers.

Each attempt will be marked after you submit your answers.

The result of your last submission will be your final marks of the quiz.

Late submissions will not be accepted for the quizzes. If you are not able to complete a quiz before its deadline, you will receive zero marks. You should ensure that you complete the quizzes ahead of the due date and time to avoid last-minute problems with technology preventing them from completing the Quizzes on time.

Referencing Style

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

Submission

Online

Learning Outcomes Assessed

- Describe key security concepts and principles
- Discuss how common security attacks and defences work
- Explain the role of cryptographic mechanisms in providing computer and network security
- Apply access control technologies, including firewalls and authentication, to secure computer networks
- Explain threats and defences that are specific to wireless networks.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Technology Competence

3 REPORT

Assessment Type

Written Assessment

Task Description

This is an individual assessment. In this assessment task, you will analyse a scenario given in this assessment item, develop and produce a written report on the given tasks. You are required to present a topic about network security in the provided scenario. This assessment includes two parts as follows:

Part A: You will draft a report for the provided scenario with the given tasks.

Part B: There will be a presentation on a topic about network security you are interested in.

The report, presentation slides and a recorded video of the presentation are due on Monday, week 13.

Assessment Due Date

Review/Exam Week Monday (10 Oct 2022) 11:45 pm AEST

This is an individual submission. All Students need to upload their report, presentation slides with the link of the recorded presentation on Moodle.

Return Date to Students

Report results with the feedbacks will be returned on the Certification of Grades Day.

Weighting

45%

Assessment Criteria

You will be assessed on your ability to analyse the given scenario and provide answers/solutions to the questions related to the case scenario.

For more details, including marking criteria, please refer to the assessment specification which can be found on the Moodle unit website.

Assignments received 14 days or more after the due date will not be marked and will receive zero.

Referencing Style

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

Submission

Online

Submission Instructions

A shared link of the recorded presentation should be inserted into the presentation slides for submission.

Learning Outcomes Assessed

- Apply access control technologies, including firewalls and authentication, to secure computer networks
- Explain threats and defences that are specific to wireless networks.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology 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