COIT20246 *Networking and Cyber Security*
Term 1 - 2024

Profile information current as at 19/05/2024 01:19 am

General Information

Overview

In this unit, you will learn how Information and Communications Technology (ICT) infrastructure supports the operation of modern organisations. You will investigate the structure of the Internet, design wired and wireless networks, and deploy applications using virtualisation and cloud computing. You will discover mechanisms for securing ICT infrastructure and applications by studying the motivation of attackers and the common vulnerabilities they exploit. You will also learn frameworks and tools organisations use to manage cloud infrastructure, reduce cyber security risks, and deliver IT services to customers. As you explore cyber security and Internet technologies via hands-on laboratory tasks, you will reflect on the impact of those technologies on society, and your responsibilities as a future ICT professional. This unit gives you the broad knowledge of networking and cyber security that all ICT professionals require and is a starting point for a career as a cyber security analyst, cloud engineer, or network operations specialist.

Details

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

Pre-requisites or Co-requisites

There are no requisites for this unit.
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
- Melbourne
- Online
- 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 6-credit Postgraduate 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. **Online Quiz(zes)**
Weighting: 35%
2. **Learning logs / diaries / Journal / log books**
Weighting: 35%
3. **Project (applied)**
Weighting: 30%

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.

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 evaluations and informal student feedback

Feedback

Students felt overwhelmed by the tutorial tasks plus regular deadlines for assessment activities.

Recommendation

Reduce the number of online quizzes, as well as the weight of draft assessments (e.g. draft journal), and provide additional guidance on amount of effort required for each task (e.g. identify what is to be included in journal for each tutorial task).

Feedback from Informal student feedback

Feedback

Some students from a non-technical background found the assessments difficult.

Recommendation

Review the assessment intructions for clarity (e.g. avoid too many technical terms, add cross-references to unit material), and provide additional videos that step through the assessments as well as demonstrate key concepts needed for the assessments.

Feedback from Teaching team feedback

Feedback

The group project was challenging, both in forming groups and ensuring team members made sufficient contributions.

Recommendation

Allocate time in tutorial classes for group formation and work on the group project, and investigate methods to encourage and monitor contributions from all team members.

Feedback from Teaching team feedback

Feedback

Project marking criteria did not provide students with enough guidance of expectations.

Recommendation

Revise the project marking criteria to include more examples of expecations at a wider range of levels (e.g. Excellent, Good, Poor).

Unit Learning Outcomes

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

1. Investigate the role of ICT infrastructure, such as computer hardware, operating systems, virtualisation, and networks, in providing Internet applications and cloud services
2. Recommend cyber security controls to prevent and detect attacks and vulnerabilities
3. Apply standards and industry best practices to manage networks, ICT services, and cyber security
4. Summarise key professional, social and legal issues relating to the Internet, cloud computing, and cyber security.

The Australian Computer Society (ACS), the professional association for Australia's ICT sector, 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 8 (the SFIA code is included):

- IT Infrastructure (ITOP)
- Network Design (NTDS)
- Network Support (NTAS)
- Information Security (SCTY)
- Security Operations (SCAD)
- Problem Management (PBMG)
- Service Level Management (SLMO)
- Change Control (CHMG)

The National Initiative for Cybersecurity Education (NICE) Framework defines knowledge, skills and tasks needed to perform various cyber security roles. Developed by the National Institute of Standards and Technology (NIST), the NICE Framework is used by organisations to plan their workforce, including recruit into cyber security positions.
This unit helps prepare you for roles such as Systems Security Analyst, Network Operations Specialist and Systems Administrator, contributing to the following knowledge and skills:

- K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0040 Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0060 Knowledge of operating systems.
- K0061 Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- K0108 Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
- K0111 Knowledge of network tools (e.g., ping, traceroute, nslookup)
- K0130 Knowledge of virtualization technologies and virtual machine development and maintenance.
- K0138 Knowledge of Wi-Fi.
- K0160 Knowledge of the common attack vectors on the network layer.
- K0200 Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
- K0318 Knowledge of operating system command-line tools.
- S0033 Skill in diagnosing connectivity problems.
- S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).

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**
1 - Online Quiz(zes) - 35%	●	●	●	
2 - Learning logs / diaries / Journal / log books - 35%	●	●		●
3 - Project (applied) - 30%			●	●

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes			
	1	**2**	**3**	**4**
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				

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)
- VirtualBox
- Wireshark
- Zoom
- Microsoft Windows on CQU Lab computer and/or personal computer
- Github.com Account
- Microsoft Teams
- Diagrams.net Drawing Software
- PowerShell
- FileZilla Client

Referencing Style

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

Teaching Contacts

David Ling Unit Coordinator
d.ling@cqu.edu.au
Steven Gordon Unit Coordinator
s.d.gordon@cqu.edu.au

Schedule

Week 1 - 04 Mar 2024		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Computer Systems and Applications		
Week 2 - 11 Mar 2024		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Computer Networks and The Internet		
Week 3 - 18 Mar 2024		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Network Technologies		
Week 4 - 25 Mar 2024		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Internetworking		
Week 5 - 01 Apr 2024		
Module/Topic	**Chapter**	**Events and Submissions/Topic**

Module/Topic	Chapter	Events and Submissions/Topic
Internet Applications		Journal Part 1 due Week 5 Tuesday 2 April 2024 9:00 AM AEST

Vacation Week - 08 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 15 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Wireless Networks		Quiz 1 will be available online in Week 6

Week 7 - 22 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Cloud Computing		

Week 8 - 29 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Attacks and Vulnerabilities		Project Part 1 due Week 8 Monday 29 April 2024 9:00 AM AEST

Week 9 - 06 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Cyber Security Management		

Week 10 - 13 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Cyber Security Controls		

Week 11 - 20 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Managing IT Services		Journal Part 2 due Week 11 Monday 20 May 2024 9:00 AM AEST

Week 12 - 27 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Careers in Networking and Cyber Security		Project Part 2 due Week 12 Monday 27 May 2024 9:00 AM AEST Quiz 2 will be in-class in Week 12

Term Specific Information

Communicating with Staff

You should use your lecture and tutorial classes as the first point of contact with teaching staff. Ask questions of your lecturer/tutor in class each week.

Outside of class times, you are encouraged to ask questions in Microsoft Teams. A link to the COIT20246 Teams site is available in the "Learning Community" tile on Moodle. You may post a question at anytime in the Teams General channel. All staff and students can see posts in the General channel, so avoid posting personal information (such as phone numbers or your assessment solutions). The teaching team will try to respond to Teams posts as soon as possible, often within an hour during work days and with an aim of within 24 hours. While response times by staff over weekends may be longer (and may not be until Monday morning), other students may respond to your question as well.

Avoid using private chat to contact staff members in Teams. Instead, post in the General channel so all staff and students can see and potentially respond to your question, and so the answer can be shared with all students. If you have a private matter that you do not want to share with others, then contact the Unit Coordinator via email. However if you ask questions about the unit content via email, then response may take longer than if using Teams, and the staff may choose to reply via Teams (so all students see the answer).

Online Accounts

You are expected to use GitHub in this unit. You will need to create an account (if you do not already have one). Instructions for doing so will be provided on Moodle.

GitHub is a website that may be hosted overseas (including the United States). In setting up an account and using for your journal and project, you will be transferring personal information to GitHub. While there is some risk in transferring your personal information overseas, we believe the benefits to you far outweigh the risk. You will gain experience using a tool widely used in industry, you will have access to tools for version control, backup, and collaboration on your resources, and will have artefacts to show to potential employers. If you have concerns with using GitHub, please contact the Unit Coordinator to discuss options.

Assessment Tasks

1 Quizzes

Assessment Type

Online Quiz(zes)

Task Description

You will undertake two (2) quizzes on Moodle throughout the term. Each quiz will cover topics leading up to that quiz and may include topics covered by previous quizzes. Typically, the quizzes will assess your knowledge of the lecture content and tutorial activities. Some questions may require you to use software, e.g., software demonstrated in lectures and/or used in tutorial activities. Each quiz will consist of multiple questions which may be of various types (e.g., multiple-choice, short answer, calculations, written text, upload a file). All quizzes are individual assessment.

Quiz 1 will be conducted online. You will have a set period of time during Week 6 to complete the quiz. There are time limits on the quiz. The quiz time limits, topics and open/close times can be found on Moodle.

Quiz 2 will be conducted in-class under the supervision of your tutor. You must attend your allocated tutorial class in Week 12 and use a lab computer to complete the quiz during class. Online students will undertake Quiz 2 in a Zoom session in Week 12 (during the scheduled Online tute). Online students will need access to a webcam, speakers, and microphone (e.g., headset).

You will not be allowed to take a quiz at any time outside of the specified open/close times unless an Assessment Extension Request is approved. In Quiz 2, if you arrive late for class, you will not be granted extra time. Changes to quiz times can only be granted with approval by the Unit Coordinator.

While quizzes will be open-book (e.g. you can use lecture slides), you will be expected to produce the answers yourself. That is, you are not allowed to communicate with others during the quiz (including other students or people online), and if you use online searches, forums or AI systems (e.g. StackExchange, ChatGPT), you are expected to write the answer in your own words. Advice on what resources can(not) be used may be provided before the start of each quiz.

You are assumed to have a working computer and Internet connection during term, and especially during times when attempting a quiz. Technical problems, such as a computer crash or loss of Internet connection, will not usually be a reason for an extra attempt or extension. You are expected to prepare your computer before the quiz starts. If problems outside of your control occur during a quiz, report immediately to your tutor, who may either extend the time or allow you to undertake the quiz at another time (with the Unit Coordinator's approval).

Number of Quizzes

2

Frequency of Quizzes
Other

Assessment Due Date

Weeks 6 and 12

Return Date to Students

One week after Quiz 1; Certification of Grades day for Quiz 2

Weighting
35%

Assessment Criteria
There are two (2) quizzes, split as follows

- Quiz 1: 10%
- Quiz 2: 25%

In most cases, quiz answers will be automatically marked, with marks awarded based on the correctness of the answer within the context of topics covered in unit. Questions may be worth different marks, with the marks shown in the quiz. If quiz answers are manually marked (e.g., explanation style questions), then marks will be awarded based on the correctness and clarity of the answer.
It is important you answer the questions within the context of this unit. There are sometimes different meanings of terms in networking and cyber security. You will be expected to use the terms as covered in the lecture materials and tutorial activities.
As results and solutions may be released shortly after the due date, late submissions are not accepted. Making no attempts before the due date will result in a score of 0.

Referencing Style

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

Submission
Online

Learning Outcomes Assessed

- Investigate the role of ICT infrastructure, such as computer hardware, operating systems, virtualisation, and networks, in providing Internet applications and cloud services
- Recommend cyber security controls to prevent and detect attacks and vulnerabilities
- Apply standards and industry best practices to manage networks, ICT services, and cyber security

2 Journal

Assessment Type
Learning logs / diaries / Journal / log books

Task Description
You will keep a journal throughout the unit that captures your tutorial activities and project contributions. Each tutorial has a set of tasks: the workings, results, answers and discussion arising from those tasks must be captured in your journal.
You must contribute to your journal every week, preferably during or shortly after each tutorial. Examples of content that may be included are:

- Screenshots capturing results of using software to complete tasks;
- Commands used to complete tasks, and the output of those commands, e.g., copy-and-paste from PowerShell;
- Network diagrams and other illustrations you develop;
- Links to websites/papers/software you used to solve problems or find information;
- Answers to questions in the tutorial activities, or relevant questions posed by your tutor or other students;
- Notes on how to use software, perform a calculation or solve a problem;
- Files you created or produced by software in conducting tutorial activities, e.g., web pages.

Tutorial activities may specify what must be included in your journal for a particular task. You should also use your journal to document your individual contributions to your project. As a general guide, include items in your journal that:

1. Provide evidence that you completed a tutorial task or made a contribution to the project (e.g., screenshots, output, commands, files, diagrams);
2. Demonstrate understanding and competence of the knowledge and skills taught (e.g., written insights, summary

3. Will be helpful for you later in the unit, or in future units, to refer back to (e.g., notes, steps you took, links to websites and other instructions).

You will have to maintain your journal such that there is evidence of regular (at least weekly) contributions. Your journal must be created in a GitHub repository created using GitHub Classroom. As this is your own journal, you should not share with other students. The journal should use basic Markdown formatting (using just plaintext or uploading a Word document is insufficient). Details of creating the GitHub repository can be found on Moodle.
You are required to submit your journal early in the term (Journal Part 1) so you can gain feedback on the suitability of your entries so far. The entire journal is then submitted towards the end of term (Journal Part 2).

Assessment Due Date

Journal Part 1 due Week 5 Tuesday 2 April 2024 9:00 AM AEST; Journal Part 2 due Week 11 Monday 20 May 2024 9:00 AM AEST

Return Date to Students

Journal Part 1 returned two weeks after submission; Journal Part 2 returned on Certification of Grades day

Weighting
35%

Assessment Criteria
Your journal is an individual assessment worth 35% of the unit assessment, split as follows:

- Journal Part 1: 10%, covering contributions from Weeks 1 to 3
- Journal Part 2: 25%, covering contributions from Weeks 4 to 10

Both parts will be marked based on the quality of the contributions (e.g., demonstrating completion and understanding of tutorial activities) and the professionalism of the contributions (e.g., weekly entries relevant to the topics in the unit and presented in a professional manner).
While the journal will be maintained on GitHub, you must also submit a ZIP of the journal on Moodle before the deadline. The ZIP file can easily be produced by exporting the repository in GitHub. This is necessary so that a permanent record of your contribution is available in Moodle (in case the online platform is not available in the future).

Referencing Style

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

Submission
Online

Submission Instructions
You must submit a ZIP of the GitHub journal onto Moodle before the deadline.

Learning Outcomes Assessed

- Investigate the role of ICT infrastructure, such as computer hardware, operating systems, virtualisation, and networks, in providing Internet applications and cloud services
- Recommend cyber security controls to prevent and detect attacks and vulnerabilities
- Summarise key professional, social and legal issues relating to the Internet, cloud computing, and cyber security.

3 Project

Assessment Type
Project (applied)

Task Description
You will conduct a project involving network design and cyber security analysis. You will apply the knowledge and skills you have learnt in the unit to propose a networking and cyber security solution for a small/medium sized organisation. You will also identify and reflect on professional and ethical issues that may arise as a result of the project. Details of the project tasks can be found on Moodle.
This is a group project consisting of two (2) students from the same class (or with the Unit Coordinators permission, three students, e.g., when an odd number of students in the class). Students should form their own groups, but if not formed within reasonable time, the Unit Coordinator may allocate students to a group. Generally, a change of groups is not allowed once the project starts. If a student is not contributing to the project (e.g., they are absent or not responding to communications), the other student must inform the Unit Coordinator as soon as possible.
Students must use a GitHub repository to track their project contributions (e.g., drafts, design files, code). Details of creating the GitHub repository can be found on Moodle. Your contributions on GitHub may be take into account when

determining your overall contribution to the project.

You will produce written reports on the project, as well as a presentation at the end of the project. The presentation will be via a recorded video. Details of the presentation format and duration can be found on Moodle.

Assessment Due Date

Project Part 1 due Week 8 Monday 29 April 2024 9:00 AM AEST; Project Part 2 due Week 12 Monday 27 May 2024 9:00 AM AEST

Return Date to Students

Project Part 1 returned two weeks after submission; Project Part 2 returned on Certification of Grades day

Weighting
30%

Assessment Criteria
Your project assessment is worth 30% of the unit assessment, split as follows:

- Project Part 1: 12%. A written report covering the network design phase.
- Project Part 2: 18%. A written report and presentation covering the entire project.

The report in both parts will be marked based on the quality of the work, the application of knowledge and skills taught in the unit, and professionalism of the report (including regular contributions to the project throughout the term, as evidenced by GitHub contributions and contributions during tutorials).

The presentation will be marked based on the ability to offer genuine, personal reflections on the project, and to clearly explain aspects of the project.

While this is a group project, some parts may be individually assessed. For example, some tasks are to be completed by the group and generally each student will receive the same marks, while some tasks will be assigned to individuals and each student will receive a mark for their assigned task. Even for the group tasks, different marks may be given to students in a group when there is a significant difference in contributions (e.g., as evidenced by GitHub contributions and contributions during tutorials).

While the project will be maintained on GitHub, you must also submit a ZIP of the project on Moodle before the deadline. The ZIP file can easily be produced by exporting the repository in GitHub. This is necessary so that a permanent record of your contribution is available in Moodle (in case the online platform is not available in the future).

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
You must submit a ZIP of the GitHub project onto Moodle before the deadline.

Learning Outcomes Assessed

- Apply standards and industry best practices to manage networks, ICT services, and cyber security
- Summarise key professional, social and legal issues relating to the Internet, cloud computing, and cyber security.

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