COIT20263 *Information Security Management*
Term 1 - 2024

Profile information current as at 05/09/2024 01:18 pm

General Information

Overview

This unit provides you with a thorough understanding of the managerial aspects of information security in a business organisation. You will complement your existing knowledge of information and communication technologies by studying the organisational and management issues relevant to information security. You will learn about the importance of information security plans, security risk management and compliance monitoring, and develop and apply security policies and best practices. Through case studies, you will consider information security strategies that support business objectives while being aware of legal and ethical obligations. As a result, you will have the knowledge and skills to contribute to information security governance in accordance with standards set by governments, professional bodies and industry.

Details

Career Level: *Postgraduate*
Unit Level: *Level 9*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites

Prerequisite: COIT20261 Network Routing and Switching
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. **In-class Test(s)**
Weighting: 30%
2. **Presentation**
Weighting: 30%
3. **Written Assessment**
Weighting: 40%

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 Self-reflection

Feedback

This unit uses examples of security policies and risk assessments from industry. Some students have difficulty in extracting key concepts from the examples and applying the concepts to write new policies.

Recommendation

Update workshops to provide students more practice of deconstructing security policies and writing security policies

Unit Learning Outcomes

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

1. Develop security policies and program for an organisations based on national and international standards and industry's best practice
2. Apply appropriate security control mechanism to protect critical infrastructure
3. Assess security risks and develop risk management strategies for an organisation
4. Justify appropriate risk treatment options
5. Integrate laws and ethics of information security management into the organisation's security framework.

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 SFIA8. The SFIA code is included:

- Information Management (IRMG)
- Information Security (SCTY)
- Risk Management (BURM);
- Continuity Management (COPL)
- Methods and Tools (METL)

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:

- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004 Knowledge of cybersecurity and privacy principles.
- K0038 Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0040 Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- K0263 Knowledge of information technology (IT) risk management policies, requirements, and procedures.
- K0267 Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- K0276 Knowledge of security management.

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				
	5				
1 - In-class Test(s) - 30%	•		•	•	•
2 - Presentation - 30%	•	•			•
3 - Written Assessment - 40%		•	•	•	

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	5				
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

COIT20263

Prescribed

MANAGEMENT OF INFORMATION SECURITY
Edition: 6th (2018)
Authors: Michael E. Whitman & Herbert J. Mattord
Cengage Learning
Boston , MA , USA
ISBN: 9781337405713
Binding: Hardcover

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- Microsoft Office Suite

Referencing Style

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

Teaching Contacts

Salahuddin Azad Unit Coordinator
s.azad@cqu.edu.au

Schedule

Week 1 - 04 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Information Security Social Engineering Attacks	Online resources supplied	

Week 2 - 11 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Security Vulnerabilities, Threats, and Countermeasures	Online resources supplied	

Week 3 - 18 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Managing Identity and Authentication	Online resources supplied	

Week 4 - 25 Mar 2024

Module/Topic	Chapter	Events and Submissions/Topic
Controlling and Monitoring Access	Online resources supplied	

Week 5 - 01 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Security Assessment and Testing	Online resources supplied	**Assessment 1** - In-class Test 1 Due: Week 5 During Tutorial

Vacation Week - 08 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
- MID-TERM BREAK -		

Week 6 - 15 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Managing Security Operations	Online resources supplied	

Week 7 - 22 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Compliance: Law and Ethics	Online resources supplied	

Week 8 - 29 Apr 2024

Module/Topic	Chapter	Events and Submissions/Topic
Security Governance, Principles and Policies	Online resources supplied	**Assessment 1** - In-class Test 2 Due: Week 8 During Tutorial

Week 9 - 06 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Risk Management Concepts (Part 1)	Online resources supplied	**Assessment 2** Due: Week 9 Monday (6 May 2024) 9:00 am AEST

Week 10 - 13 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Risk Management Concepts (Part 2) Personnel Security	Online resources supplied	

Week 11 - 20 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Protecting Security of Assets	Online resources supplied	**Assessment 1** - In-class Test 3 Due: Week 9 During Tutorial

Week 12 - 27 May 2024

Module/Topic	Chapter	Events and Submissions/Topic
Preventing and Responding to Incidents	Online resources supplied	**Assessment 3** - Oral Assessment Due: Week 12 During Tutorial **Assessment 3** Due: Week 12 Monday (27 May 2024) 9:00 am AEST

Review/Exam Week - 03 Jun 2024

Module/Topic	Chapter	Events and Submissions/Topic

Exam Week - 10 Jun 2024

Module/Topic	Chapter	Events and Submissions/Topic
No final exam in this unit		

Term Specific Information

Contact information for Dr Salahuddin Azad:

Email: s.azad@cqu.edu.au; Office: Level 6, 120 Spencer Street, Melbourne Vic 3000; P +61 3 9616 0680 | X 50680.

If you have any queries, please email me and I will get back to you within one business day or so. For an individual discussion, please ring me during business hours (or leave a message if I am not in) and I will return your call as soon as possible.

The following book will be used as an supplementary textbook:

Chapple, M. Stewart, J. M. and Gibson D. (2021). *Certified Information Systems Security Professional Official Study Guide*. 9th ed. Sybex.

Assessment Tasks

1 Assessment 1

Assessment Type
In-class Test(s)

Task Description
This is an **individual** assessment.

In this assessment, there will be three in-class tests: In-class Test 1, In-class Test 2, and In-class Test 3 in **Week 5**, **Week 8**, and **Week 11**. Each in-class test will carry 10 marks.

The in-class tests will assess your knowledge and understanding of security vulnerabilities, countermeasures, security controls, security assessments, managing security operations, risk assessments, risk management frameworks, security governance, policies, and ethics, laws and compliance.

In each in-class test, you will first complete an online quiz on Moodle during the tutorial. Afterwards, your tutor will interview individual students to check their understanding. Online students will be contacted by the Unit Coordinator to schedule in-class tests via Zoom. In that case, it will be mandatory to have your webcam on during the whole session.

Further detail of this assessment will be provided on the Moodle unit website.

Assessment Due Date

In-class Test 1 will be conducted in Week 5, In-class Test 2 will be conducted in Week 8, and In-class Test 3 will be conducted in Week 11.

Return Date to Students

The marks and feedback will be returned within 2 weeks after the completion of respective in-class test.

Weighting
30%

Assessment Criteria
This assessment will assess your knowledge and understanding of security vulnerabilities, countermeasures, security controls, security assessments, managing security operations, risk assessments, risk management frameworks, security governance, policies, and ethics, laws and compliance.

The detailed marking criteria will be provided on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
You will individually complete three in-class quizzes via Moodle.

Learning Outcomes Assessed

- Develop security policies and program for an organisations based on national and international standards and industry's best practice
- Assess security risks and develop risk management strategies for an organisation
- Justify appropriate risk treatment options
- Integrate laws and ethics of information security management into the organisation's security framework.

2 Assessment 2

Assessment Type
Presentation

Task Description
This is a **group** assessment. Students must form teams of at least **3 students** and a maximum of 4 students, with any larger teams at the discretion of the Unit Coordinator.

For this assessment, you are required to work in a group to develop and deliver a presentation on an information security topic. You will be provided a list of topics to choose from for your presentation. You will conduct research on the chosen topic and present your findings in the presentation.

The presentations will be conducted during the tutorials in **Week 9** and **Week 10**. Online students will be contacted by the Unit Coordinator to schedule presentations via Zoom. When the presentation is conducted via Zoom, it is mandatory to have your webcam on during the presentation. The presentation file must be submitted to Moodle by **Monday Week 9**.

Further detail of this assessment will be provided on the Moodle unit website.

Assessment Due Date
Week 9 Monday (6 May 2024) 9:00 am AEST

The presentation file must be submitted to Moodle by the above due date and time.

Return Date to Students
Week 11 Monday (20 May 2024)

The marks and feedback will be returned within 2 weeks after the submission due date.

Weighting
30%

Assessment Criteria
This assessment will assess your knowledge on security risks, security controls, security governance, policies, and ethics, laws and compliance, and capacity to apply that knowledge .

The detailed marking criteria will be provided on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each of you in the group must submit the same presentation file to Moodle as a .ppt file.

Learning Outcomes Assessed

- Develop security policies and program for an organisations based on national and international standards and industry's best practice
- Apply appropriate security control mechanism to protect critical infrastructure
- Integrate laws and ethics of information security management into the organisation's security framework.

3 Assessment 3

Assessment Type
Written Assessment

Task Description
This is a **group** assessment. Students must form teams of at least **3 students** and a maximum of 4 students, with any larger teams at the discretion of the Unit Coordinator.

There are two parts of this assessment task - Part A and Part B. It is mandatory to attempt both parts to complete this assessment.

Part A: Written Report
For this part, you will be required to produce a written report, completing a few tasks on the security controls, security risk assessment and risk treatment. You may need to apply international standards such as NIST Cybersecurity Framework, or ISO/IEC standards to produce your report. The written report is due on **Monday Week 12**.

Although this is a group assessment, the marks might vary based on the individual contribution. In your final report, you need to clearly provide information regarding each group members contribution, peer evaluation of group members contribution, and reflection on your group experience.

Part B: Oral Assessment
There will be an oral assessment on the written report, during which you will need to answer questions about your written report verbally. The purpose of the oral assessment is to clarify the your understanding of the written report. For on-campus students, the viva will be conducted face-to-face during the tutorial in **Week 12**. Online students will be contacted by the Unit Coordinator to schedule a oral assessment session. When the oral assessment is conducted via Zoom, it is mandatory to have your webcam on during the conversation.

Further details of this assessment task will be provided on the Moodle unit website.

Assessment Due Date
Week 12 Monday (27 May 2024) 9:00 am AEST

The written report must be submitted to Moodle by the above due date and time.

Return Date to Students

The marks and feedback will be returned on the day of certification of grades.

Weighting
40%

Assessment Criteria
This assessment will assess your knowledge on risk assessments, security controls, and capacity to apply appropriate risk treatment options .

The detailed marking criteria will be provided on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each of you in the group must submit the same written report to Moodle as a Microsoft Word file.

Learning Outcomes Assessed

- Apply appropriate security control mechanism to protect critical infrastructure
- Assess security risks and develop risk management strategies for an organisation
- Justify appropriate risk treatment options

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