COIT20263 *Information Security Management*
Term 2 - 2023

Profile information current as at 28/04/2024 12:05 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 2 - 2023

- 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. **Written Assessment**
Weighting: 35%
2. **Group Discussion**
Weighting: 25%
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. Analyse the information security policies and programs of organisations based on national and international standards
2. Develop the guidelines for an information security policy for an organisation
3. Apply information security risk standards to protect information assets in organisations
4. Justify information security certification and accreditation required in relation to personnel and information security of an organisation
5. Compare and contrast the laws and ethics of information security management.

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 online tool MySFIA to build their 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 Management (IRMG)
- Information Security (SCTY)
- Business Risk Management (BURM);
- Continuity Management (COPL)
- Project Management (PRMG)
- 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				
	1	2	3	4	5
1 - Written Assessment - 35%		•			
2 - Group Discussion - 25%	•				•
3 - Written Assessment - 40%			•	•	

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	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

Additional Textbook Information
This book is available to view online at the CQUni Library at no charge. Limited paper copies at a reduced price can be purchased at the CQUni Bookshop: 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)
- 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

Md Hossain Unit Coordinator
m.m.hossain@cqu.edu.au

Schedule

Week 1 - 10 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to the Management of Information Security	Online resources supplied	Group discussion

Week 2 - 17 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Governance and Strategic Planning for Security	Online resources supplied	Continuation of Group Discussion

Week 3 - 24 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Information Security Policy	Online resources supplied	Continuation of Group Discussion

Week 4 - 31 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic

Compliance: Law and Ethics	Online resources supplied	Continuation of Group Discussion

Week 5 - 07 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Developing the Security Program	Online resources supplied	Continuation of Group Discussion. **Assessment Item 1** Due: Week 5 Friday (11 Aug 2023) 11:45 pm AEST

Vacation Week - 14 Aug 2023

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

Week 6 - 21 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Risk Management: Assessing Risk	Online resources supplied	Continuation of Group Discussion

Week 7 - 28 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Risk Management: Treating Risk	Online resources supplied	Continuation of Group Discussion. **Assessment Item 2 - Part 1**: Group submission (workshops of weeks 4 and 5) due on week 7 Friday 11:45 PM AEST.

Week 8 - 04 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Security Management Models	Online resources supplied	Continuation of Group Discussion

Week 9 - 11 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Security Management Practices	Online resources supplied	Continuation of Group Discussion

Week 10 - 18 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Planning for Contingencies	Online resources supplied	Continuation of Group Discussion **Assessment Item 2 - Part 2**: Group submission (workshops of weeks 8, 9 and 10) due on Week 10 Friday 11:45 PM AEST.

Week 11 - 25 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Security Maintenance	Online resources supplied	Continuation of Group Discussion

Week 12 - 02 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
Protection Mechanisms	Online resources supplied	Continuation of Group Discussion.

Review/Exam Week - 09 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
		Assessment Item 3 Due: Review/Exam Week Tuesday (10 Oct 2023) 11:45 pm AEST

Exam Week - 16 Oct 2023

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

Term Specific Information

Unit Coordinator: Dr Md Monir Hossain
Email:m.m.hossain@cqu.edu.au

Assessment Tasks

1 Assessment Item 1

Assessment Type
Written Assessment

Task Description
This is an individual assessment.
This assessment relates to the Unit Learning Outcome 2. You will analyse the scenario given in this assessment item, develop and produce a written report on the guidelines for the given information security policy. Further details of this assessment task will be provided on the Moodle unit website.

Assessment Due Date
Week 5 Friday (11 Aug 2023) 11:45 pm AEST
Individual submission via Moodle link

Return Date to Students
Week 7 Monday (28 Aug 2023)
Online. Two weeks after the due date or two weeks after submission, whichever is later.

Weighting
35%

Assessment Criteria
You are assessed mainly on your ability to analyse the given scenario and develop the guidelines for the given information security policy. Please see the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each student must submit to Moodle their written report as a Microsoft Word file.

Learning Outcomes Assessed

- Develop the guidelines for an information security policy for an organisation

2 Assessment Item 2

Assessment Type
Group Discussion

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.
Several tasks based on the given case study will be provided in class during your weekly workshops. Answers should be maintained in a portfolio document (e.g. a simple A4 - word document, Online Portfolio, etc).
This assessment has two submission parts:

- Part 1- Weeks 4 and 5 exercises by Friday 11:45 PM of Week 7. This part is worth 10%.
- Part 2- Weeks 8, 9 and 10 exercises by Friday 11:45 PM of Week 10. This part is worth 15%.

Assessment Due Date

Part 1 is due on Friday 11:45 PM of week 7. Part 2 is due on Friday 11:45 PM of week 10. Both via Moodle.

Return Date to Students

Two weeks after the due date or two weeks after submission, whichever is later.

Weighting
25%

Assessment Criteria
Marking for each individual workshop exercise will be based on: discussion, relevance, and clarity/effort.
Details of the marking schedule will be available on the Moodle unit website.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Part 1 is due on Friday 11:45 PM of week 7. Part 2 is due on Friday 11:45 PM of week 10. Both parts should be submitted via Moodle.

Learning Outcomes Assessed

- Analyse the information security policies and programs of organisations based on national and international standards
- Compare and contrast the laws and ethics of information security management.

3 Assessment Item 3

Assessment Type
Written Assessment

Task Description
This is a group assessment.
This assessment task relates to the Unit Learning Outcomes 3 and 4. You will produce a written report on the guidelines of information security risk management as well as information security certification and accreditation for the organisation in the given scenario of this assessment item. Further details of this assessment task will be provided on the Moodle unit website.

Assessment Due Date
Review/Exam Week Tuesday (10 Oct 2023) 11:45 pm AEST
Each of you in the group must upload the same written report to Moodle as a Microsoft Word file by the above due date.

Return Date to Students

On Certification Day.

Weighting
40%

Assessment Criteria
You are assessed on your ability to apply the principles of information security risk management as well as information security certification and accreditation to the organisation in the given scenario. Please see the Moodle unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each of you in the group must upload the same written report to Moodle as a Microsoft Word file by the above due date.

Learning Outcomes Assessed

- Apply information security risk standards to protect information assets in organisations
- Justify information security certification and accreditation required in relation to personnel and information security of an organisation

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