COIT20263 *Information Security Management*
Term 1 - 2017

Profile information current as at 29/04/2024 09:04 am

General Information

Overview

This advanced management unit provides postgraduate networks and information security students with a thorough understanding of the concepts, processes and controls for the assurance of information security within a business organisation. The unit builds on student's prior knowledge of the measures associated with the protection of an organisation's information infrastructure assets and the most cost-effective and appropriate ways of planning and implementing these measures. Drawing on the fundamental premise that information security is a management issue, and not a technical one alone, the unit covers areas of information security planning, governance, policies, best practices, risk management, compliance, personnel, law and ethics. The unit qualifies the student to apply the gained knowledge and skills to real world situations, and 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 - 2017

- Brisbane
- Distance
- Melbourne
- 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. **Group Discussion**
Weighting: 15%
2. **Practical and Written Assessment**
Weighting: 35%
3. **Group Discussion**
Weighting: 10%
4. **Practical and 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 Student Course Evaluations.

Feedback
Most students are happy with the course.

Recommendation
Keep the course content and the assessment tasks as they are.

Action
Unit content and the format of assessment tasks were kept as they were.

Feedback from Student Course Evaluations.

Feedback
Distance students should be able to form groups with on-campus students.

Recommendation
This was possible even now. Include a statement in the assessment task that distance students can form groups with on-campus students.

Action
A statement was included in assessment tasks that the distance students can form groups with on-campus students.

Unit Learning Outcomes

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

1. Explain how information security management fits into general business management.
2. Analyse the information security domain both in respect of security policy and security application.
3. Examine the dominant information security blueprints, methods, processes and models, within the framework of national and international standards.
4. Research emerging trends in the certification and accreditation of information security systems in Australia and other countries.
5. Analyse various risk theories and how these will be applied to the protection of information assets.
6. Critically evaluate and reflect on ethical issues that relate to the practice of information security.
7. Compare and contrast current laws, regulations, and relevant professional organisations.

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)
- Data Management (DATM)
- Methods and Tools (METL)

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	7
1 - Group Discussion - 15%				•			•
2 - Practical and Written Assessment - 35%	•	•					
3 - Group Discussion - 10%			•				
4 - Practical and Written Assessment - 40%					•	•	

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes						
	1	2	3	4	5	6	7
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							

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes							
	1	2	3	4	5	6	7	8
1 - Group Discussion - 15%	○	○		○	○	○		
2 - Practical and Written Assessment - 35%	○	○	○	○				
3 - Group Discussion - 10%	○	○	○		○			
4 - Practical and Written Assessment - 40%	○	○	○	○				

Textbooks and Resources

Textbooks

COIT20263

Prescribed

Management of Information Security
Edition: 5th (2017)
Authors: Michael E. Whitman & Herbert J. Mattord
Cengage Learning
Stamford , Connecticut , USA
ISBN: 9781305501256
Binding: Hardcover

Additional Textbook Information

It is recommended that students purchase the electronic version of this book (e-book). The e-book should be purchased directly from the Publisher. To do so:

1. Browse to www.cengagebrain.com

2. Search for the book "Management of Information Security" by Whitman & Mattord, 5th edition (as detailed above).

3. From the purchase options displayed, select the e-book version. Purchasing the e-book gives 6-months access to the e-book, according to the site.

4. If you have any questions about the e-book, you need to contact the Publisher directly using the contact details given on the publisher's website.

5. If no questions, then go ahead and purchase the e-book directly from the site.

NOTE: If you prefer the printed version of the book, contact the CQU Bookshop (+61 7 4930 9421) in the first instance.

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)

Referencing Style

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

Teaching Contacts

Rohan De Silva Unit Coordinator
r.desilva@cqu.edu.au

Schedule

Week 1 - 06 Mar 2017

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to the Management of Information Security	1	
Week 2 - 13 Mar 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Compliance: Law and Ethics	2	
Week 3 - 20 Mar 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Governance and Strategic Planning for Security	3	Start of Group Discussion I
Week 4 - 27 Mar 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Information Security Policy	4	Continuation of Group Discussion I
Week 5 - 03 Apr 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Developing the Security Program	5	End of Group Discussion I
Vacation Week - 10 Apr 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
- MID-TERM BREAK -		
Week 6 - 17 Apr 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Risk Management: Identifying and Assessing Risk	6	**Group Discussion I** Due: Week 6 Friday (21 Apr 2017) 11:30 pm AEST
Week 7 - 24 Apr 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Risk Management: Controlling Risk	7	**Written Assessment 1** Due: Week 7 Friday (28 Apr 2017) 11:30 pm AEST
Week 8 - 01 May 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Security Management Models	8	Start of Group Discussion II
Week 9 - 08 May 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Security Management Practices	9	Continuation of Group Discussion II
Week 10 - 15 May 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Planning for Contingencies	10	End of Group Discussion II **Group Discussion II** Due: Week 10 Friday (19 May 2017) 11:30 pm AEST
Week 11 - 22 May 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Personnel and Security	11	**Written Assessment 2** Due: Week 11 Friday (26 May 2017) 11:30 pm AEST
Week 12 - 29 May 2017		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
Protection Mechanisms	12	

Review/Exam Week - 05 Jun 2017

Module/Topic	Chapter	Events and Submissions/Topic

Exam Week - 12 Jun 2017

Module/Topic	Chapter	Events and Submissions/Topic

Term Specific Information

Contact information for Dr Rohan de Silva:
Email: r.desilva@cqu.edu.au Telephone: (02) 9324 5748 Office: Level 6, 400 Kent Street, Sydney Campus. Please submit questions about the course through the 'Q&A' discussion forum in Moodle, so that everyone can benefit from the questions and answers. If you have any individual queries, please email me and I'll try to get back to you within a day or so. For an individual discussion, please phone during work hours (leave a message if I'm not in and I'll return your call as soon as I can).

Assessment Tasks

1 Group Discussion I

Assessment Type
Group Discussion

Task Description
This assessment task has a group discussion and a video presentation of the outcome of the discussion. In their groups of up to 4 members, the students will discuss the enterprise information security policy issues of the organisation in the given scenario in relation to the Unit Learning Outcomes 4 and 7. The students need to contribute to their group discussion in Group Discussion I Forum in Moodle during weeks 3, 4 and 5. Each student should copy/paste their discussions to a Word document and upload the latter to Moodle by the deadline in Week 6. Also, they need to individually prepare and upload a very brief video (5 min max.) to YouTube and provide the link in the Word document. Distance students can form groups with on-campus students as well. Further details of this assessment task will be provided on the Moodle unit webpage.

Assessment Due Date
Week 6 Friday (21 Apr 2017) 11:30 pm AEST
Contributions during each week from weeks 3-5 should be concluded by 11.30 pm, Friday of the respective week. The contributions of each student should be copy/pasted to a Word document and uploaded to Moodle by the above deadline. Recorded video presentation should be uploaded to YouTube and the link to the video should be provided in the Word document.

Return Date to Students
Week 8 Friday (5 May 2017)

Weighting
15%

Assessment Criteria
In this assessment task, the students are assessed against their ability to discuss the enterprise information security issues of the organisation in the given scenario in relation to the Unit Learning Outcomes 4 and 7. Please see the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each student has to contribute to Group Discussion I Forum of their group in Moodle each week. The contributions of each student should be copy/pasted to a Word document and uploaded to Moodle by the above deadline. Recorded video presentation should be uploaded to YouTube and the link to the video should be provided in the Word document.

Learning Outcomes Assessed

- Research emerging trends in the certification and accreditation of information security systems in Australia and other countries.
- Compare and contrast current laws, regulations, and relevant professional organisations.

Graduate Attributes

- Knowledge
- Communication
- Research
- Self-management
- Ethical and Professional Responsibility

2 Written Assessment 1

Assessment Type
Practical and Written Assessment

Task Description
This assessment task relates to the Unit Learning Outcomes 1 and 2, and can be undertaken in a group of up to 4 members or individually. Each student will analyse the given scenario and develop an information security policy, either individually or through discussions with other students in their group. Distance students can form groups with on-campus students as well. Further details of this assessment task will be provided on the Moodle unit webpage.

Assessment Due Date
Week 7 Friday (28 Apr 2017) 11:30 pm AEST
The written report should be uploaded to Moodle by each student by the above due date.

Return Date to Students
Week 9 Friday (12 May 2017)

Weighting
35%

Assessment Criteria
The students are assessed against their ability to analyse the given scenario and develop an information security policy. Please see the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each student has to upload the written assignment as a Microsoft Office Word file to Moodle.

Learning Outcomes Assessed

- Explain how information security management fits into general business management.
- Analyse the information security domain both in respect of security policy and security application.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research

3 Group Discussion II

Assessment Type
Group Discussion

Task Description
In their groups of up to 4 members, the students will discuss the information security risk management issues of the organisation in the given scenario in relation to the Unit Learning Outcome 3. The students need to contribute to their group discussion in Group Discussion II Forum in Moodle during weeks 8, 9 and 10. Each student should copy/paste their discussions to a Word document and upload it to Moodle by the deadline in Week 10. Distance students can form groups with on-campus students as well. Further details of this assessment task will be provided on the Moodle unit webpage.

Assessment Due Date
Week 10 Friday (19 May 2017) 11:30 pm AEST
Contributions during each week from weeks 8-10 should be concluded by 11.30 pm, Friday of the respective week. The contributions of each student should be copy/pasted to a Word document and uploaded to Moodle by the above deadline.

Return Date to Students
Week 12 Friday (2 June 2017)

Weighting
10%

Assessment Criteria
In this assessment task, the students are assessed against their ability to discuss the information security risk management issues of the organisation in the given scenario in relation to the Unit Learning Outcome 3. Please see the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each student has to contribute to the Group Discussion II Forum of their group in Moodle each week. The contributions of each student should be copy/pasted to a Word document and uploaded to Moodle by the above deadline.

Learning Outcomes Assessed

- Examine the dominant information security blueprints, methods, processes and models, within the framework of national and international standards.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Self-management

4 Written Assessment 2

Assessment Type
Practical and Written Assessment

Task Description
This assessment task relates to the Unit Learning Outcomes 5 and 6, and can be undertaken in a group of up to 4 members or individually. The students will need to apply the principles of information security risk management to the organisation in the given scenario and produce a written report. Distance students can form groups with on-campus students as well. Further details of this assessment task will be provided on the Moodle unit webpage.

Assessment Due Date
Week 11 Friday (26 May 2017) 11:30 pm AEST
The written report should be uploaded to Moodle by each student by the above due date.

Return Date to Students

On Certification Day.

Weighting
40%

Assessment Criteria
The students are assessed against their ability to apply the principles of information security risk management to the organisation in the given scenario. Please see the unit website for more specific marking criteria.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Each student needs to upload the written report to Moodle as a Microsoft Office Word file.

Learning Outcomes Assessed

- Analyse various risk theories and how these will be applied to the protection of information assets.
- Critically evaluate and reflect on ethical issues that relate to the practice of information security.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research

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