Faculty of Science, Engineering and Built Environment

SIT284 Cyber Security Management

Deakin University Unit Guide

Trimester 2, 2019

CONTENTS

WELCOME

Welcome to the **Cyber Security Management (SIT284)** unit. This is an introductory unit on information and enterprise security from a management perspective. The primary emphasis will be on assessing security needs and deployment of electronic business securely. This is one of the core units for the students who want to specialise in the computer security stream.

The primary focus of this unit provides students with a broad view of information security threat, planning for information security, risk analysis, security policies, models, and mechanisms for ensuring confidentiality, integrity, and availability of information assets. I hope that you enjoy studying this unit. The resources contained within the unit site, accessed in DeakinSync, together with the prescribed textbook, forms the assessable content for this unit. Please take the time to familiarise yourself with the content provided on the unit site.

The Resource Map link on the unit site home page will provide you with a list of the resources contained within this section and where they are located. Please begin your study by examining the Unit Outline document, located on the CloudDeakin unit home page. It is important that you read this document as information varies between units and over trimesters. Among other information, you will find a list of staff members and their contact details should you have any queries, assessment requirements, breakdowns, and due dates, and prescribed texts.

I hope you have an enjoyable and challenging trimester.
Good luck

Professor Jemal Abawajy and Dr Morshed Chowdhury

This Unit Guide provides you with the key information about this Unit. For the best chance of success, you should read it very carefully and refer to it frequently throughout the trimester. Your Unit site (accessed in **DeakinSync**) also provides information about your **rights and responsibilities.** We will assume you have read this before the Unit commences, and we expect you to refer to it throughout the trimester.

WHO IS THE UNIT TEAM?

Unit chair: leads the teaching team and is responsible for overall delivery of this unit

Jemal Abawajy

Unit chair details

Campus:	Geelong Waurn Ponds Campus Pigdons Road GEELONG VIC 3217
Email:	jemal.abawajy@deakin.edu.au
Phone:	+61 3 522 71376

Other members of the team and how to contact them

Burwood Campus Leader: contact the campus leader for assistance at your campus

Name: Dr Morshed Chowdhury, Senior Lecturer and Campus Coordinator

Email: morshed.chowdhury@deakin.edu.au
Phone: +61 3 925 17478

Administrative queries

- Contact your Unit Chair or Campus Leader
- Drop in or contact Student Central to speak with a Student Adviser

For additional support information, please see the Rights and Responsibilities section under 'Resources' in your unit site

ABOUT THIS UNIT

This unit provides students with the foundations required to learn cyberspace safety and security, and security management at corporate level. In SIT284 students will learn how security assessment is methodologically and procedurally conducted with business operational constraints. Students will examine both business and security operations. The unit enables students to develop contingency planning, risk assessment, risk management and compliance standards for various businesses. The key focus of SIT284 is on introducing students to IT security policy development and human security management. Students will also explore legal and ethical issues in the context of security management and audit.

Unit development in response to student feedback

Every trimester, we ask students to tell us, through eVALUate, what helped and hindered their learning in each Unit. You are strongly encouraged to provide constructive feedback for this Unit when eVALUate opens (you will be emailed a link).

In previous versions of this unit, students have told us that these aspects of the Unit have helped them to achieve the learning outcomes:

- The lecturers were very patient with students and took the time to help them with their misunderstandings; demonstrate patience and respectful guidance when interacting with students.
- Content was developed very well.

They have also made suggestions for improvement, and so this is what we have done:

- We plan to ask students to form their own group in the first instance. After a certain time period, we will assign students to groups randomly.
- Lecture slides used by Burwood and Geelong/Cloud lecturers will be largely the same.

If you have any concerns about the Unit during the trimester, please contact the unit teaching team - preferably early in the trimester - so we can discuss your concerns, and make adjustments, if appropriate.

Your course and Deakin's Graduate Learning Outcomes

GLO1	Discipline knowledge and capabilities:	appropriate to the level of study related to a discipline or profession
GLO2	Communication:	using oral, written and interpersonal communication to inform, motivate and effect change
GLO3	Digital literacy:	using technologies to find, use and disseminate information

GLO4	Critical thinking:	evaluating information using critical and analytical thinking and judgment
GLO5	Problem solving:	creating solutions to authentic (real world and ill-defined) problems
GLO6	Self-management:	working and learning independently, and taking responsibility for personal actions
GLO7	Teamwork:	working and learning with others from different disciplines and backgrounds
GLO8	Global citizenship:	engaging ethically and productively in the professional context and with diverse communities and cultures in a global context

Each Deakin course has **course learning outcomes** which explain what the Deakin Learning Outcomes mean in your discipline. Learning in each unit builds towards the course learning outcomes.

Your Unit Learning Outcomes

Each Unit in your course is a building block towards these Graduate Learning Outcomes - not all Units develop and assess every Graduate Learning Outcome (GLO).

	These are the Learning Outcomes (ULO) for this Unit **At the completion of this Unit, successful** students can:	Deakin Graduate Learning Outcomes
ULO1	Work as a team and apply organisational planning and project management principles to IT security planning.	GLO1, GLO4, GLO7
ULO2	Assess security risks, threats and vulnerabilities to the organisation and implement appropriate information security protection mechanisms.	GLO1, GLO4, GLO5
ULO3	Conduct investigation of security management issues in organisation by analysing requirements, plans and IT security policies.	GLO1, GLO4, GLO5
ULO4	Identify personnel security, training and security education needs, and associated legal and ethical awareness and propose strategies for corporations taking into account cost benefit ratios.	GLO1, GLO4, GLO5

ASSESSING YOUR ACHIEVEMENT OF THE UNIT LEARNING OUTCOMES

Overview

In brief, these are the assessment tasks for this Unit (details below):

Group planning report 30%, case investigation report 20%, examination 50%

Summative assessments

(tasks that will be graded or marked)
NOTE: It is <u>your responsibility</u> to keep a backup copy of every assignment where it is possible (eg written/digital reports, essays, videos, images). In the unusual event that one of your assignments is misplaced, you will need to submit the backup copy. Any work you submit may be checked by electronic or other means for the purposes of detecting collusion and/or plagiarism.

When you are required to submit an assignment through your unit site (accessed in DeakinSync), you should receive an email to your Deakin email address confirming that it has been submitted. You should check that you can see your assignment in the Submissions view of the Assignment folder after upload, and check for, and keep, the email receipt for the submission.

- Summative assessment task 1

	Case investigation report
Brief description of assessment task	This assessment is for students to conduct investigation of serious security management issues in corporate organisations. Students will be required to apply prescribed management and audit procedures as well as analysis of roles, duties and privileges. They will be required to prepare a security management report based on the findings of their investigation and by using knowledge of IT security policies, risk assessment and risk management processes. Students are also required to identify personnel security, training, security education needs, and associated legal and ethical awareness.
Detail of student output	This is an individual assessment task. Students are required to submit a case investigation report of approximately 2000 words along with exhibits to support findings and a list of bibliography. This report should consist of: • an overview of the IT security management case • list of risks, threats and possible countermeasures • analysis of findings • review and reflection on the findings and propose justified recommendations
Grading and weighting (% total mark for unit)	20%, numerically marked.
This task assesses your achievement of these Unit Learning Outcome(s)	ULO2 Assess security risks, threats and vulnerabilities to the organisation and implement appropriate information security protection mechanisms. ULO3 Conduct investigation of security management issues in organisation by analysing requirements, plans and IT security policies. ULO4 Identify personnel security, training and security education needs, and associated legal and ethical awareness and propose strategies for corporations taking into account cost benefit ratios.
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 through the assessment of student knowledge of standard procedures and ethical codes to be followed in security management GLO4 through the assessment of student ability to reflect and critically analyse business information and security issues to further probe information GLO5 through the assessment of student competence in conducting security analysis and audit
How and when you will receive feedback on your work	Students should reflect on the feedback provided to them from the assessment task 1. Further, ongoing feedback will be provided during practical sessions to aid analysis, documentation and problem solving techniques.
When and how to submit your work	Case investigation report submission should be made electronically via the unit site (accessed in DeakinSync) and is due by Monday 5 August 2019 (week 5) at 5:00PM (AEST).

- Summative assessment task 2

	Group planning report
Brief description of assessment task	This assessment is for students to demonstrate their ability to plan an investigation of security management issues in corporate organisations. Students are required to work as a team and use IT security planning and project management principles to plan an IT security investigation and management project. They will be required to follow prescribed procedures to evaluate the risk levels, potential impact of threats and vulnerabilities, and cost-benefit analysis of control methods. Student teams will be tested on their ability to analyse the security objectives of businesses and requirements and propose justified contingency plans to manage security risks.
Detail of student output	This is a group assessment task. Student teams must prepare a report of approximately 2500 words and must include: • description of the targeted IT environment; • a detailed analysis of the corporate environment; and • plan for approaching the identification of security threats
Grading and weighting (% total mark for unit)	30%, numerically marked. While this is a team task that generates a single team mark, students will receive individual marks based upon their contribution to the task determined via self and peer assessment and unit chair assessment of their teamwork skills.
This task assesses your achievement of these Unit Learning Outcome(s)	ULO1 Work as a team and apply organisational planning and project management principles to IT security planning. ULO2 Assess security risks, threats and vulnerabilities to the organisation using critical thinking and problem solving techniques and tools for planning
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 through the assessment of student knowledge of standard procedures to be followed in security management GLO4 through the assessment of student ability to reflect and critically analyse constraints and business requirements for conducting security analysis. GLO5 through the assessment of student ability in conducting security analysis and proposing a plan/solution. GLO7 through the assessment of students' teamwork skills in planning an investigation..
How and when you will receive feedback on your work	Students will have the opportunity to seek regular feedback during the weekly practical sessions to deepen their knowledge and to rectify misunderstandings and misinterpretation. Feedback provided for this report will be useful for implementing the testing plan in the following assessment task.
When and how to submit your work	Planning report submission should be made electronically via the unit site (accessed in DeakinSync), and is due by Monday 16 September 2019 (week 10) at 5:00 PM (AEST)

- Summative assessment task 3

	Examination
Brief description of assessment task	This closed book examination will assess student's knowledge of security analysis, security management, methods to minimize the risks and procedures to security audit. Students must demonstrate an ability to relate, analyse and respond to questions around IT security management and audit under examination conditions..
Detail of student output	Written closed-book exam paper which needs at least 500 words to answer.
Grading and weighting (% total mark for unit)	50%
This task assesses your achievement of these Unit Learning Outcome(s)	ULO2 Assess security risks, threats and vulnerabilities to the organisation and implement appropriate information security protection mechanisms. ULO3 Conduct investigation of security management issues in organisation by analysing requirements, plans and IT security policies. ULO4 Identify personnel security, training and security education needs, and associated legal and ethical awareness and propose strategies for corporations taking into account cost benefit ratios.
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 through assessment of student knowledge of security analysis, security management, methods to minimize risks and procedures to audit security GLO5 through assessment of student ability to conduct security management analysis by following prescribed procedures
How and when you will receive feedback on your work	Feedback provided to students in practical sessions focuses on information security management. Students are also required to undertake a guided research case studies underpinning security management and audit for modern businesses. Feedback and student reflection on these activities will be relevant for enhanced student performance in the examination.
When and how to submit your work	Students will be required to attend a supervised examination during the end of trimester examination period. It is the responsibility of students to review their examination timetable when it is released via DeakinSync.

Your learning experiences in this Unit - and your expected commitment

To be successful in this unit, you must:

- Read all materials in preparation for your classes or seminars, and follow up each with further study and research on the topic;
- Start your assessment tasks well ahead of the due date;
- Read or listen to all feedback carefully, and use it in your future work;
- Attend and engage in all timetabled learning experiences as follows:

Scheduled learning activities - campus

2 x 1 hour classes per week, 1 x 2 hour practical per week.

Scheduled learning activities - cloud

1 x 1 hour scheduled online workshop per week.

Students will on average spend 150 hours over the trimester undertaking learning and assessment activities for this unit. For campus students this includes class time as described, designated activities in the practical sessions, assessment tasks, readings and study time. For cloud students the time should be divided between online learning activities, discussion boards, designated activities in the practical sessions, assessment tasks, readings and study time.

Most of the studying materials including class slides and practical instructions will be hosted on the unit site. Assignment instructions will be posted on the unit site approximately two weeks before the due dates. Most of the practical sessions will be conducted in virtual machine environment, which is hosted by the school of IT's VM clusters; the instructions of using VM will be introduced during practical sessions in week 1.

This unit has a prescribed textbook. Please refer to the table in the Unit Weekly Activities section below for the teaching schedule. You should read the relevant chapters before the class in which it is covered.

Note

At Deakin,

- *Lectures* are referred to as *classes* (definition: a general meeting for all students, for which students do not need to register and where students are engaged through presentations and learning activities)
- *Tutorials, workshops and seminars* are referred to as seminars (definition: more interactive meetings for smaller groups of students).
- For the complete list of agreed definitions for learning experiences, see the Course Design and Delivery Procedure.

UNIT LEARNING RESOURCES

Your unit learning resources are available in your unit site accessed in DeakinSync.

Prescribed text

Whitman, © 2019, Management of Information Security, 6th edition, Cengage Learning

Essential learning resources

See above prescribed text.

Textbooks, reference books, general books and software may be ordered from the bookshop:
phone 1800 686 681 (freecall);
email to DUSA-Bookshop@deakin.edu.au; or
order online from the University bookshop web site at http://www.dusabookshop.com.au/

Recommended learning resources

Suitable reference books for this unit include:

- Harold F. Tiopton and Micki Krause, Information Security Management Handbook, 2003. 5th Edition, Auerbach Publications. ISBN 0-8493-1997-8
- Information Technology Security & Risk Management, 2006, John Wiley & Sons. Australia Ltd. ISBN 0-470-80574-9
- Reading and Cases in the Management of Information Security, Thomson, Course Technology, 2006. ISBN 0-619-21627-1
- Linda Volonino and Stephen R. Robinson, Principals and Practice of Information Security, 2004, Prentice Hall. ISBN 0-1-

-184027-4

- Michael E. Whitman and Herbert J. Mattord, "Management of Information Security" Thomson, Course Technology, 2004. ISBN 0-619-21515-1

KEY DATES FOR THIS TRIMESTER

Trimester begins (classes begin)	Monday 8 July 2019
Intra-trimester break (a short break during trimester)	Monday 12 August - Sunday 18 August 2019
Trimester ends (classes cease)	Thursday 26 September 2019
Study period (examination preparation period)	Monday 30 September - Friday 4 October 2019
Examinations begin	Monday 7 October 2019
Examinations end	Friday 18 October 2019
Inter-trimester break (the period between trimesters)	Monday 21 October - Friday 8 November 2019
Unit results released	Thursday 7 November 2019 (6pm)

UNIT WEEKLY ACTIVITIES

Week	Commencing	Topic	Assessment activity
1	8 July 2019	Introduction to Management of Information Security (Chapter 1)	
2	15 July	Compliance: Law and Ethics (Chapter 2)	
3	22 July	Governance and Strategic Planning for Security (Chapter 3)	
4	29 July	Information Security Policy (Chapter 4)	
5	5 August	Developing the Security Program (Chapter 5)	
6	19 August	Risk Management: Identifying and Assessing Risk (Chapter 6)	Case Investigation Report
7	26 August	Risk Management: Controlling Risk (Chapter 7)	
8	2 September	Security Management Models and Practices (Chapter 8 and Chapter 9)	
9	9 September	Planning for Contingencies (Chapters 10)	
10	16 September	Protection Mechanisms (Chapter 12)	Group Planning Report
11*	23 September	Review	

Intra-trimester break: **Monday 12 August - Sunday 18 August 2019** (between weeks 5 and 6)
***Friday 27 September:** AFL Grand Final Eve public holiday - University closed