



# ACCG878

## Fraud Examination, Investigative Techniques

S2 External 2019

*Dept of Accounting & Corporate Governance*

### Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	3
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	3
<u>Delivery and Resources</u>	7
<u>Unit Schedule</u>	10
<u>Learning and Teaching Activities</u>	13
<u>Policies and Procedures</u>	14
<u>Graduate Capabilities</u>	17
<u>Changes from Previous Offering</u>	20
<u>Research and Practice, Global and Sustainability</u>	20

#### Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

## General Information

Unit convenor and teaching staff

Unit Convenor

Verity Greenwood

[verity.greenwood@mq.edu.au](mailto:verity.greenwood@mq.edu.au)

Contact via [verity.greenwood@mq.edu.au](mailto:verity.greenwood@mq.edu.au)

E4A 310

Wednesday 2.00pm- 4.00pm or by appointment

Moderator

Hope Ashiabor

[hope.ashiabor@mq.edu.au](mailto:hope.ashiabor@mq.edu.au)

Contact via N/A

N/A

N/A

Credit points

4

Prerequisites

(4cp in ACCG or ACST or BUS or ECON or MKTG units at 600 level) or admission to MCyberSec

Corequisites

Co-badged status

Unit description

This unit is a partner in the Association of Certified Fraud Examiners (ACFE) Anti-Fraud Education Partnership. The unit is designed to provide practical knowledge and skills to manage appropriate responses required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises. Corporate compliance and action programs with legislative requirements will be addressed as well as fraud and corruption risk assessments that assist discovery, identification and reporting of corporate wrongdoing. In particular, this program enables practitioners to effectively retrieve and secure documentary or other evidence to support fraud investigations. Students will appreciate the composition of the investigation team and the issues and challenges that need to be addressed to successfully manage a fraud investigation.

## Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are

available at <https://www.mq.edu.au/study/calendar-of-dates>

## Learning Outcomes

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

Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.

Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.

Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.

Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## General Assessment Information

### Assessment Criteria

Three criteria will be used to assess student work in this Unit:

- Knowledge Development: Understanding of key ideas, knowledge components and their interrelationships.
- Application: Ability to apply theoretical ideas and frameworks to educational practice in a critically reflective way.
- Presentation: The extent to which the work has been written and presented in a manner consistent with accepted academic standards

The ACCG878 Assessment Guide discusses fully the performance against the standards in relation to each of these criteria.

## Assessment Tasks

Name	Weighting	Hurdle	Due
<a href="#">Online Forum</a>	20%	No	19/08/2019-22/08/2019
<a href="#">Reflective Task (RT)</a>	20%	No	5.00pm 15/09/19
<a href="#">Case Investigation Report</a>	60%	No	5pm 10/11/2019

## Online Forum

Due: **19/08/2019-22/08/2019**

Weighting: **20%**

Detail regarding the Online Forum is provided in the the Assessment Guide and discussed in the Module One seminar. In summary the topics is:

### Online Forum

#### Responding to the Allegations

#### Assessed

#### Topic:

Internet fraud is not committed by computers but father by the fraudsters using them. However, technology is a vital aspect of a wrongdoers' schemes and the efforts to catch them. For further details, see Module 1.

Detail regarding the Online Forum is provided in *Relationship between Assessment and Learning Outcomes* in the Unit Assessment Guide (pages 13-14). **Note that non-submission into the Forum will result in an automatic fail grade for the missed Online Forum assessment.**

On successful completion you will be able to:

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## Reflective Task (RT)

Due: **5.00pm 15/09/19**

Weighting: **20%**

The Reflective Task has a definite topic based on the unit case study, your contributions are

assessed and feedback is given. Details of the Reflective Task are provided for each Module and will be discussed in the seminars. In summary the topics are:

## **Reflective Task**

### **Modules 1 and 2**

#### **Assessed**

##### **Topic:**

'Fraudsters seek to exploit the everyday routines of daily living and the functioning of institutions, using technology as an adaptive threat, which can change its target, timing, and mode of delivery as circumstances are altered.'

**Submission:** The deadline for the Reflective Task are provided in the Assessment Guide under the heading *Relationship between Assessment and Learning Outcomes (pages 13-14 of that guide)*. The RT is to be submitted by 5pm on the 15th September, 2019 (due date). Online submission will be subject to Turn-it-in check (Maximum 500 words). Ensure that the statement on page 3 under 'General Assessment Information' is cut and pasted into your RT. This statement will not be included in your word count. Also ensure that the RT is uploaded and submitted correctly by clicking the 'submit' button. Documents left as drafts on the submission site will not be marked.

**Penalty:** There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late (for example, 25 hours late in submission – 20% penalty). This penalty does not apply for cases in which an application for Special Consideration is made and approved. No submission will be accepted after any solutions have been posted.

**Extension:** No extensions will be granted unless approval has been given under the Special Consideration Policy.

On successful completion you will be able to:

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## Case Investigation Report

Due: **5pm 10/11/2019**

Weighting: **60%**

In Week 1, a 'real life' case study scenario, the 'Serenity Valley' case study, will be given. This 'Serenity Valley' case study will be used in a logical flow as the basic model for the fraud investigation in all the modules covered in the unit. The case investigation report is based on the findings of the 'Serenity Valley' fraud investigation case study used in the unit. Consequently, gathering evidence in a portfolio for the report should be a continuing feature of your participation in the unit. A fraud examiner is responsible for writing clear, accurate and unbiased reports reflecting the fraud investigation and fraud examination results. The suggested structure of the finished Case Investigation Report is in the ACCG878 Assessment Guide.

**Submission :** Case Investigation Report is to be submitted by 5pm on Sunday 10 November, 2019. This assignment is to be a concise word processed document (maximum 3,000 words) and English expression is very important in this task. Online submission will be subject to a Turn-it-in check. Ensure that the statement on page 3 under 'General Assessment Information' is cut and pasted into your case investigation report. This statement will not be included in your word count. Also ensure that the case investigation report is uploaded and submitted correctly by clicking the 'submit' button. Documents left as drafts on the submission site will not be marked.

**Penalty and Extension:** No extensions will be granted. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late (for example, 25 hours late in submission – 20% penalty). This penalty does not apply for cases in which an application for special consideration is made and approved. No submission will be accepted after solutions have been posted.

**Note that non-submission of the assignment will result in an automatic fail grade for the unit.**

On successful completion you will be able to:

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## Delivery and Resources

### Unit web page

Course material is available on the Macquarie University learning management system (ilearn). The web page for this unit can be found at <http://mq.edu.au/iLear/index.htm>

The unit is divided into three specific Modules, each Module will cover a specific set of topics as listed in the Unit Schedule. Each Module provides opportunities to explore concepts covered through discussions and group activities. The unit is delivered online through recorded lecture seminars and materials, online webinars; 'convenor chat' and email. The recorded lecture seminars will be delivered as an ECHO recording and as a specific video recorded lecture. The mode of delivery for each topic is listed in the unit schedule of this unit guide.

The timetable for classes can be found on the University web site at:

<http://www.timetables.mq.edu.au/>

### Live Webinars

Live webinar sessions will provide opportunities to explore concepts covered in each Module through discussions and group activities. The dates/times for each webinar is listed in the unit guide. Details regarding access and password to log in to the webinar will be posted on the 'Discussion forum prior to each scheduled webinar. Attendance in the webinar is strongly encouraged.

### Prescribed texts

De Kauwe, Shane (2018) *The Law of Fraud: An Australian Investigator's Guide*, Critical Mass, Newtown, ISBN 9781925786200 (Available in Co-op and Macquarie Library Reserve).

Jackson, C.W. *Detecting Accounting Fraud: Analysis and Ethics*, Global Edition, Pearson Publishers, ISBN 10: 1292059400/ ISBN 13: 9781292059402 (Available in Co-op and in Macquarie Library Reserve)

Silverstone, H., Sheetz, M. Pednault, S. and Rudewicz, F (2012) *Forensic Accounting and Fraud Investigation for Non-Experts*, 3<sup>rd</sup> Ed, John Wiley & Sons, New Jersey, USA (Electronic version available Macquarie Library e-Reserve HV8079.F7.S55 2012)

### Prescribed legislation

Commonwealth Government, *Corporations Act 2001* (Corporations Act) Part 9.4AAA Section 1317 AA-AE, [http://www.comlaw.gov.au/Details/C2013C00003/Html/Volume\\_5#\\_Toc344127819](http://www.comlaw.gov.au/Details/C2013C00003/Html/Volume_5#_Toc344127819)

*Corporations Act 2001* (Corporations Act) Part 9.4AAA Section 1317 AA-AE (Cth) [www.comlaw.gov.au/Details/C2013C00003/Html/Volume\\_5#\\_Toc344127819](http://www.comlaw.gov.au/Details/C2013C00003/Html/Volume_5#_Toc344127819)

*Cybercrime Act 2001*, No. 161, 2001 (Cth) <https://www.legislation.gov.au/Details/C2004A00937>

*Cybercrime Legislation Amendment Act 2012*, No. 120, 2012 (Cth) <https://www.legislation.gov.au/Details/C2012A00120>

*Independent Commission Against Corruption Act 1988* No 35. <http://www.legislation.nsw.gov.au/>



[maintop/view/inforce/act+35+1988+cd+0+N](#)

New South Wales Government, *Public Interest Disclosures Act* 1994 No 92, <http://www.legislation.nsw.gov.au/viewtop/inforce/act+92+1994+FIRST+0+N/>

*Privacy and Personal Information Protection Act* 1998, [http://www.austlii.edu.au/au/legis/nsw/consol\\_act/papipa1998464/](http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/)

Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2019, <https://www.legislation.gov.au/Details/C2019A00010>

## Recommended Books

Meyer, P. (2010) *Liespotting: Proven Techniques to Detect Deception*, St. Martins Griffin, New York (Available Macquarie Library).

Pednault, S. (2010) *Anatomy of a Fraud Investigation: from detection to prosecution*, John Wiley & Sons, Inc. Hoboken, New Jersey (Available Macquarie Library).

Rabon, D. and Chapman, C. (2010) *Fraud –Related Interviewing*, Carolina Academic Press, Durham, North Carolina(Available Macquarie Library).

Wells, J.T. (2017) *Corporate Fraud Handbook: Prevention and Detection*, 5th Edition. ISBN: 978-1-119-35198-6 ((Electronic version available Macquarie Library e-Reserve)

## Recommended Journal

Ó Ciardhuáin, S. (2004) An Extended Model of Cybercrime Investigations, *International Journal of Digital Evidence*, Summer 2004, Vol 3, Issue 1, <https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf>

A module-by-module list of the topics to be covered is at the end of the unit guide.

Component	Details
Unit Outline	Read this Unit Outline right through first. It contains a great deal of information that you'll need to know, including assessment requirements and grading criteria, schedules of activities, reading guidelines and information about plagiarism, progress and where to get help.
Modules	There are three Modules in this Unit. The three provide summaries of content, suggested readings, assessment Tasks (readings and associated questions to help guide your study) and information about the online Forum and other assessments. See the next Section for details.
Online Forum	One formal online Forum will be conducted during the Session. This is analogous to tutorials in a traditional course. You are required to participate actively in it, and your contributions will be assessed. There is an informal 'Discussion Forum' (not assessed!), allowing opportunities for postings by the Convenor and discussions and requests for help from classmates which might take place outside a traditional class. For example, if you want to meet online with a few classmates to swap drafts of your evolving report and get their help, the 'Discussion Forum' is a good place to do it.
Reflective Task Assessment	One Reflective Task (RT) assessment will be conducted. You are required to complete and submit this assessment online and your assessment will be assessed. The Reflective Task is an exercise designed to encourage reflection on Unit topics and associated readings. For details of RT and how it is assessed, see <i>Relationship between Assessment and Learning Outcomes</i> section, ACCG878 Assessment guide. Online submission subject to Turn-it-in check.



<b>Live Webinars</b>	There are also live Webinars. These are informal discussion forums, allowing opportunities for the kind of activities listed under 'Live Webinar' in each Module in the Unit Schedule of this unit guide.
<b>Consultations</b>	Attend the Convenor consultations in E4A 310, 4 Eastern Road when you need to discuss the unit or seek further assistance as required. Consultations with the Convenor can also be arranged outside the specified consultation times upon request.
<b>e-Reserve</b>	Recommended readings can be downloaded from e-Reserve. The e-reserve link gives you access to other areas of the library that you will need, namely the Journal Finder, Catalogue and Databases.

## Overview of Modules

An overview of modules is given below:

Module	Provides opportunities for participants to:
<b>Module 1</b> <b>Responding to the Allegations</b>	<ul style="list-style-type: none"> <li>• recognise the different types of fraud and the assessment criteria for fraud</li> <li>• appreciate the impact of components of the fraud diamond</li> <li>• develop an effective fraud policy and understand the merits of a fraud risk management program</li> <li>• Perform cyber security governance 'health checks' to assist an organisation understand its cyber security strengths and weaknesses</li> <li>• understand the first steps that organisations and fraud examiners should take when an allegation of fraud arises</li> <li>• understand the requirements for whistleblower protection.</li> </ul>
<b>Module 2</b> <b>Fraud Investigation Team</b>	<ul style="list-style-type: none"> <li>• design the structure of the investigation team</li> <li>• identify skills required to conduct an investigation</li> <li>• understand the selection process for fraud investigation team members</li> <li>• develop understanding of the challenges in managing the fraud examination team</li> </ul>
<b>Module 3</b> <b>Investigative Techniques</b>	<ul style="list-style-type: none"> <li>• outline a fraud investigative course of action</li> <li>• identify phases, tasks and checkpoints in a fraud investigation</li> <li>• address planning, managing and monitoring the investigation and the investigation team</li> <li>• understand the importance of balancing conflicting resources and time management</li> <li>• demonstrate written and oral communication skills relevant to an appropriate professional environment.</li> </ul>

## Work Requirements

This Unit has been designed as a 4 postgraduate credit point Unit, requiring the equivalent of 13 weeks of work over one semester. Being a four credit-points Unit you should expect to spend a minimum of 12 hours per week to meet the requirements of the Unit. As a postgraduate student, you bring valuable knowledge and experience to the Unit. As you work through the Unit, try to:

- critically question your own preconceptions
- share your insights with others in the group
- contribute to critical analysis and debate of concepts found in the literature and the views of other class members.

In completing the Unit, you are expected to:

- participate fully in the online forum and in webinars
- provide feedback in the webinars
- create a fraud investigation portfolio based on the 'Serenity Valley' case study
- read at least the material in e-reserve and any other materials designated for each module, and bring this reading into webinar discussions.

### **Assignment Preparation and Submission**

At the start of each assignment submitted online (Reflective Task and Case Investigation Report), you are required to paste in the following words and insert your name:

I, **[Insert your name]**, declare that:

This assignment is entirely my own work based on my personal study and/or research.

- I have acknowledged all material and sources used in the preparation of this assignment, including any material generated in the course of my employment .
- I have not copied in part, or in whole, or otherwise plagiarised, the work of others.
- The assignment, or substantial parts of it, has not previously been submitted for assessment in any formal course of study in this or any other institution, unless acknowledged in the assignment and previously agreed to by the Unit's Convenor
- The assignment is within the word and page limits specified for the assignment
- The use of any material in this assignment does not infringe the intellectual property / copyright of a third party
- I understand that this assignment may undergo electronic detection for plagiarism and a copy of the assignment may be retained on the University's database and used to make comparisons with other assignments in the future
- All written work must be submitted as Microsoft Word files. When naming files please adopt the following convention, and this wording should also appear on each page of the Assignment : eg **ACCG878 John Smith RT1**

## **Unit Schedule**

Module 1: Responding To The Allegations

Topic/ Subsection	Readings and activities	Online delivery (Recorded video seminars and ECHO)	Live Webinar 1.00pm 14.8.19 : (Access and password will be posted on the unit website prior to webinar event).
1.1 Introduction		Introduction to unit.	
1.2 Introduction to Internal Fraud Investigations	1. Read Jackson (2015) Ch.1-3; 2. Read Silverstone <i>et al</i> (2012) Ch.2,pp.17-29 3. Pre -read 'Serenity Valley' case study (Part 1).	Impact/prevalence of Fraud; Fraud diamond; Organisation fraud management policy; Identification of Fraud and third party risk.	1. Introduction of 'real life' Serenity Valley' case study 2. Discuss responses to Peter Madoff Case Study a. and b. (page 64) with your discussion group
1.3 Legal Context of Internal Investigations	1. Refer to legislation listed under 'Prescribed and Recommended texts and/or materials Readings List 2. Read De Kauwe, Ch. 3,pp. 3-31; Ch. 5, pp 64-83.	Review relevant fraud legislation/legal framework of cyber security; court system; new whistleblower legislation.	
1.4 Finding Fraud	1. Read Jackson (Ch 4) 2. Read Silverstone et al (2012) Ch.7 3. Read D Kauwe, Ch. 33, pp.32-56. 4. Read Serenity Valley case study (Parts 2 and 3).	Reactive Fraud Investigation; Signs of Fraud; Looking for Suspects; Evaluating Fraud Tips; Confronting Suspects; Audits and Investigations.	1. Prepare answer to Peregrine case study a (1) and b. and discuss with your discussion group. 2. Discuss Serenity Valley case study Parts 2 and 3.
1.5 Initial Assessment and Procedure	1. Read De Kauwe, Ch. 8,p. 116; Ch. 9 pp. 117-122. 2. Read Silverstone et al (2012) Ch.9, pp.143 -156	Key elements of investigation; investigation protocol; response and process upon allegation of fraud	
<b>Module 2: Fraud Examination Team</b>			
Topic/ Subsection	Readings and activities	Online delivery (Recorded video seminars and ECHO)	Live Webinar 4.00pm 11.9.19 (Access and password will be posted on the unit website prior to webinar event).

2.1 <b>Managing The Case</b>	1. Read Silverstone <i>et al</i> (2012) Ch.9, pp.160-167 2. Read Serenity Valley case study Part 4.	*Industry Lecturer*  Insights into managing and assessing engagement with victim organisation;  meeting of the minds;  budget and cost control; protocols;  mapping work and supervision.	1. Discuss seminar 1.5 and 2.1. 2. Discuss Serenity Valley case study Part 4.
2.2 <b>Managing The Fraud Investigation Team</b>	1. Read De Kauwe, Ch. 10, pp. 123-125. 2. Suggested reading: Pednault 2010 (Ch 2) 3. Read Serenity Valley case study Part 5.	Structuring/identifying skills and expertise of fraud investigation team; allocation/management of resources; investigation process	Discuss Serenity Valley case study Part 5.
2.3 <b>Project Management</b>	1. Read De Kauwe, Ch. 4, pp. 164-165. 2. Read Jackson, Ch. 5; 3. Read Serenity Valley case study Part 6 and 7.	Recorded seminar:  Identifying phases, tasks and checkpoints; dealing with under performing team members; monitoring progress and balancing resources.	Prepare answers for Tyco International case study (p.179) and discuss with your group
2.4 <b>Professional Standards</b>	1. Read De Kauwe, Ch. 12, pp. 129-130 2. Read Jackson, Ch. 8 'Effective Practices for Managing Conflicts of Interest (pp. 307-310).	Internal/external expertise; Conflicts of interest; Reporting issues; Investigation objectives; Ethical and moral practice.	
<b>Module 3: Investigative Techniques</b>			
<b>Topic/ Subsection</b>	<b>Readings and activities</b>	<b>Online delivery</b> (Recorded video seminars and ECHO)	<b>Live Webinar 1.00pm 23.10.19</b> (Access and password will be posted on the unit website prior to webinar event).
3.1 <b>Electronic Investigation and Surveillance</b>	1. Read Silverstone <i>et al</i> (2012) Ch. 9, pp.145-163, Ch 12 2.Suggested reading Pednault (2010), Ch.5	Electronic Investigation, Surveillance and Matrices Design	Use provided matrix to highlight individual relationships, activities, roles, positions, social links/ relationships. Cross check against posted convenor matrix.

<b>3.2</b>  <b>Document Collection and Analysis</b>	1. Read De Kauwe, Ch. 14, pp.158-163. 2. Read Silverstone <i>et al</i> (2012) Ch. 11 3. Suggested reading Pednault (2010), Ch.7 4. Read Ó Ciardhuáin, S. (2004) 5. Read Serenity Valley case study Parts 8 & 9.	*Guest Lecturer*  Recorded seminar:  Securing digital and physical documentary evidence.	
<b>3.3</b>  <b>Interviewing Witnesses and Suspects</b>	1. Read De Kauwe, Ch. 12 pp.128-132; Ch. 13, pp. 133-157. 2. Read Silverstone <i>et al</i> (2012) Ch.10 3. Suggested reading: Rabon & Chapman (2010) 4. Read Serenity Valley case study Parts 10 and 11.	Recorded seminar:  Defining a lie; lie detection skills; deception motives; semantics; interview suspect/ witnesses approach and tips; interview mistakes.	Download Serenity Valley case study suspect interview and locate 10 tell-tale signs of deception. Discuss your results with your group.
<b>3.4</b>  <b>Reporting and Litigation</b>	1. Read De Kauwe, Ch. 15, pp. 166-175. 2. Read Silverstone <i>et al</i> (2012) Ch.14 3. Suggested reading Pednault (2010), Ch.12 4. Read Ch 7 (Jackson) pp.277-278 . 5. Read Serenity Valley case study Part 12.	Case study resolution, reflection and remediation; expert witness requirements; litigation process	
<b>3.5</b>  <b>Case Investigation Report Summary</b>		Review of case investigation report and assessment requirements.	

## Learning and Teaching Activities

### Review topics, pre-read and prepare for assigned activities

Case study: Throughout the unit delivery it is expected that each Part of the Serenity Valley case study will be read and added to the case study portfolio. Preparation and review of academic literature : prior to each Module online delivery session students will be expected to have pre-read the required readings and some articles listed in the Suggested Readings list and contribute

to the online discussion forum (Live Webinar) concerning various aspects under each topic designated for that particular Module. Group discussions: A list of the required readings for each Module/topic is covered at the end of the unit guide.

## Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central](https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central) (<https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central>). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- [Academic Appeals Policy](#)
- [Academic Integrity Policy](#)
- [Academic Progression Policy](#)
- [Assessment Policy](#)
- [Fitness to Practice Procedure](#)
- [Grade Appeal Policy](#)
- [Complaint Management Procedure for Students and Members of the Public](#)
- [Special Consideration Policy](#) (**Note:** *The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.*)

Undergraduate students seeking more policy resources can visit the [Student Policy Gateway](https://students.mq.edu.au/support/study/student-policy-gateway) (<https://students.mq.edu.au/support/study/student-policy-gateway>). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit [Policy Central](https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central) (<https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central>).

## Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: <https://students.mq.edu.au/study/getting-started/student-conduct>

## Results

Results published on platform other than [eStudent](#), (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in [eStudent](#). For more information visit [ask.mq.edu.au](https://ask.mq.edu.au) or if you are a Global MBA student contact [globalmba.support@mq.edu.au](mailto:globalmba.support@mq.edu.au)

### Extensions

You are expected to submit written assessment tasks by the published due date UNLESS you have received written permission to submit your work at a later date from the Unit convenor. Extensions will only be granted in exceptional, unforeseen circumstances (known workload is not a legitimate or sufficient reason for the granting of an extension). However, Special

Consideration is available for students who are prevented by serious and unavoidable disruption from completing any Unit requirements in accordance with their ability. All students have the right to submit an application for Special Consideration. Details of how the University defines serious and unavoidable disruption to studies, and information about the processes involved, are contained in the [Special Consideration Policy](#).

### **Confidentiality**

In the actual and virtual classroom, the University respects your right to confidentiality and to having your ideas protected. We aim to develop a safe and secure online learning environment in which you can freely express your ideas and opinions. Your Unit convenor will ensure that all submitted online discussions and assignments are treated with confidentiality and respect.

The password-protected component of your Unit's web site is hosted on Online Learning @ MQ. For information about confidentiality when studying online, see <http://online.mq.edu.au/uw/conf.html>

Note that submission of assignments via iLearn involves an inbuilt automatic check for plagiarism using the Turnitin application.

### **Academic Honesty**

The nature of scholarly endeavour, dependent as it is on the work of others, binds all members of the University community to abide by the principles of academic honesty. Its fundamental principle is that all staff and students act with integrity in the creation, development, application and use of ideas and information. This means that:

- all academic work claimed as original is the work of the author making the claim
- all academic collaborations are acknowledged
- academic work is not falsified in any way
- when the ideas of others are used, these ideas are acknowledged appropriately.

Further information on the academic honesty can be found in the Macquarie University Academic Honesty Policy at University Academic Honesty Policy at [http://www.mq.edu.au/policy/docs/academic\\_honesty/policy.html](http://www.mq.edu.au/policy/docs/academic_honesty/policy.html)

### **Grades**

Macquarie University uses the following grades in coursework units of study:

HD –High Distinction

D – Distinction

CR – Credit

P – Pass

F – Fail

Grade descriptors and other information concerning grading are contained in the Macquarie University Grading Policy which is available at:



<http://www.mq.edu.au/policy/docs/grading/policy.html>

All final grades in the Department of Accounting and Corporate Governance are determined by a grading committee and are not the sole responsibility of the Unit Coordinator.

The final grade that is awarded reflect the corresponding grade descriptor in the Grading Policy.

To pass the unit, students need an overall mark of 50%.

### **Grading appeals and final examination script viewing**

If, at the conclusion of the unit, you have performed below expectations, and are considering lodging an appeal of grade and/or viewing your final exam script please refer to the following website which provides information about these processes and the cut off dates in the first instance. Please read the instructions provided concerning what constitutes a valid grounds for appeal before appealing your grade. These are available at [http://www.businessand economics.mq.edu.au/for/new\\_and\\_current\\_students/undergraduate current students/how do i/grade\\_appeal](http://www.businessand economics.mq.edu.au/for/new_and_current_students/undergraduate_current_students/how_to_grade_appeal)

### **Student Support Services**

Macquarie University provides a range of Academic Student Support Services. Details of these services can be accessed at <http://www.student.mq.edu.au>.

### **IT Conditions of Use**

Access to all student computing facilities within the Faculty of Business and Economics is restricted to authorised coursework for approved units. Student ID cards must be displayed in the locations provided at all times.

Students are expected to act responsibly when utilising University IT facilities. The following regulations apply to the use of computing facilities and online services:

- Accessing inappropriate web sites or downloading inappropriate material is not permitted. Material that is not related to coursework for approved unit is deemed inappropriate.
- Downloading copyright material without permission from the copyright owner is illegal, and strictly prohibited. Students detected undertaking such activities will face disciplinary action, which may result in criminal proceedings.

Non-compliance with these conditions may result in disciplinary action without further notice.

Students must use their Macquarie University email addresses to communicate with staff as it is University policy that the University issued email account is used for official University communication.

## **Student Support**

Macquarie University provides a range of support services for students. For details, visit <http://students.mq.edu.au/support/>

## **Learning Skills**

Learning Skills ([mq.edu.au/learningskills](http://mq.edu.au/learningskills)) provides academic writing resources and study strategies to improve your marks and take control of your study.

- [Workshops](#)
- [StudyWise](#)
- [Academic Integrity Module for Students](#)
- [Ask a Learning Adviser](#)

## Student Services and Support

Students with a disability are encouraged to contact the [Disability Service](#) who can provide appropriate help with any issues that arise during their studies.

## Student Enquiries

For all student enquiries, visit Student Connect at [ask.mq.edu.au](http://ask.mq.edu.au)

If you are a Global MBA student contact [globalmba.support@mq.edu.au](mailto:globalmba.support@mq.edu.au)

## IT Help

For help with University computer systems and technology, visit [http://www.mq.edu.au/about\\_us/offices\\_and\\_units/information\\_technology/help/](http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/).

When using the University's IT, you must adhere to the [Acceptable Use of IT Resources Policy](#). The policy applies to all who connect to the MQ network including students.

## Graduate Capabilities

### PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

### Learning outcomes

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## Assessment tasks

- Online Forum
- Reflective Task (RT)
- Case Investigation Report

## Learning and teaching activities

- Case study: Throughout the unit delivery it is expected that each Part of the Serenity Valley case study will be read and added to the case study portfolio. Preparation and review of academic literature : prior to each Module online delivery session students will be expected to have pre-read the required readings and some articles listed in the Suggested Readings list and contribute to the online discussion forum (Live Webinar) concerning various aspects under each topic designated for that particular Module. Group discussions: A list of the required readings for each Module/topic is covered at the end of the unit guide.

## PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

## Learning outcomes

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## Assessment tasks

- Online Forum

- Reflective Task (RT)
- Case Investigation Report

## **Learning and teaching activities**

- Case study: Throughout the unit delivery it is expected that each Part of the Serenity Valley case study will be read and added to the case study portfolio. Preparation and review of academic literature : prior to each Module online delivery session students will be expected to have pre-read the required readings and some articles listed in the Suggested Readings list and contribute to the online discussion forum (Live Webinar) concerning various aspects under each topic designated for that particular Module. Group discussions: A list of the required readings for each Module/topic is covered at the end of the unit guide.

## **PG - Research and Problem Solving Capability**

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

## **Learning outcomes**

- Demonstrate an understanding of the key legislation relating to fraud and cybercrime and the legal principles underpinning the definition of criminal behaviour.
- Analyse the appropriate response and steps required to be taken by organisations, fraud examiners and individuals when an allegation of fraud arises.
- Appreciate the composition of the investigation team, the rationale for the inclusion of each individual and the issues and challenges that need to be addressed to successfully manage a fraud investigation conducted by teams.
- Apply a framework of logic and inference to secure digital or physical documentary evidence, identify relationships, prepare an investigative report, understand the role and nature of witness testimony and implement a cyber governance framework in an organisation.

## **Assessment tasks**

- Online Forum
- Reflective Task (RT)
- Case Investigation Report

## Learning and teaching activities

- Case study: Throughout the unit delivery it is expected that each Part of the Serenity Valley case study will be read and added to the case study portfolio. Preparation and review of academic literature : prior to each Module online delivery session students will be expected to have pre-read the required readings and some articles listed in the Suggested Readings list and contribute to the online discussion forum (Live Webinar) concerning various aspects under each topic designated for that particular Module.  
Group discussions: A list of the required readings for each Module/topic is covered at the end of the unit guide.

## Changes from Previous Offering

The unit is a core unit in the Master of Cybersecurity, Cyber Governance and Management specialisation. Therefore, the modules include an emphasis on performing cyber security governance 'health checks' to assist an organisation understand its cyber security strengths and weaknesses. The ongoing real life 'Serenity Valley' case study is underpinned by a cyber crime scenario.

Assessments are designed to correlate and reflect the three modules in the unit. There is one Online Forum (20%) and only one Reflective Task (weighting 30%).

Live webinars are designed to assist increased online discussion amongst external students and with the Convenor.

Prescribed and recommended reading list includes legislation, books and journals relating to cyber security.

## Research and Practice, Global and Sustainability

1. This Unit has been designed as a 4 postgraduate credit point Unit, requiring the equivalent of 13 weeks of work over one session. Being a four credit-points Unit you should expect to spend a minimum of 12 hours per week to meet the requirements of the Unit. As a guide students should spend the approximate amounts of time as listed on each of the following activities (Note: Each activity listed includes hours required for pre-reading and self-study):

	Activities	Hours
1	3 online Module sessions	50
2	Assessment Task 1 (1 Online Forum)	20
3	Assessment Task 2 (1 Reflective Task)	20
4	Assessment Task 3 (Final Case Study)	60
	TOTAL	150

As a postgraduate student, you bring valuable knowledge and experience to the Unit. As

you work through the Unit, try to:

- critically question your own preconceptions
- share your insights with others in the group
- contribute to critical analysis and debate of concepts discussed in the Modules, found in the literature and the views of other class members.

In completing the Unit, you are expected to:

- participate fully in online

Forums

- provide feedback in the live webinars
- read at least one of the texts as set out for each module on the unit website and be prepared to discussing this reading in the live webinars.

2. This unit holds an Anti-Fraud Education Partnership with the *Association of Certified Fraud Examiners (ACFE)*.

3. This unit gives you opportunities to conduct research combined with practical expertise with regard to the Online Forum and Reflective Task. Further information on the Forum and Reflective Task is provided in the Assessment guide.

This unit addresses global and sustainability issues as direct areas of study and as necessary implications arising from the materials, assessment and academic discussion and debate in classes. We promote sustainability by developing ability in students to research and locate information within accounting discipline. We aim to provide students with an opportunity to obtain skills which will benefit them throughout their career.

The unit materials have a reference list at the end and within each module/text containing all references cited by the author. These provide some guidance to references that could be used to research particular issues.

4. The unit uses **recent research by the Unit Convenor:**

Verity Greenwood and Larry Dwyer (2017) 'Reinventing Macau tourism: gambling on creativity?' *Current Issues in Tourism*, Vol. 20, 6, pp. 580-602.

Greenwood, Verity A. 'Navigating Evolving Global Trends in Financial Crime: a Tourism Focus', *BESTEN Think Tank*, Berlin, 13 July 2016.

Greenwood, V and Larry Dwyer (2015) Consumer protection legislation: A neglected determinant of destination competitiveness? *Journal of Hospitality and Tourism Management* 09/201

Greenwood, V and Larry Dwyer (2014) 'Challenges to Consumer Protection Legislation in Tourism Contexts' *Journal of Tourism Consumption and Practice*, Vol. 6, 2.  
<http://www.tourismconsumption.org/current.htm>.

5. The convenor/ lecturer is affiliated with the following organisations:

- Association of Certified Fraud Examiners (ACFE) (Director, ACFE Sydney Chapter)
- Australian Legal Teacher's Association (ALTA)
- Transparency International Australia (TI)
- Australian Information Security Association (AISA)

- Association for American Geographers (AAG)
- Council for Australasian University Tourism and Hospitality Education (CAUTHE).

5. This unit uses research from external sources:

See the prescribed and recommended reading list in above and Seminar activity instructions.