



COURSE OUTLINE

SEC703 Complex Cyber Investigations Management

Course Coordinator: Clive Harfield (charfiel@usc.edu.au) **School:** School of Science, Technology and Engineering

2021 | Semester 2

Online

ONLINE

You can do this course without coming onto campus.

Please go to the USC website for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

Cyber investigation managers must plan and execute investigations into various genres of digitized deviancy, identifying and securing physical and witness evidence as well as digital evidence. Good management practice includes understanding digital deviancy; recognizing the demands of investigation as a profession; and managing processes such as systemic thinking, decision making, risk recognition, and resource allocation. This online course will introduce you to the complexities surrounding investigation decision-making processes, definitions of digital deviancy, as well as the limits and boundaries of investigative procedures and methodologies.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
ONLINE 1			
Online – The course is delivered via online materials and tutorial classes managed synchronously online. Learners are expected to spend 10-12 hours per week studying this course.	10hrs	Week 1	13 times

1.3. Course Topics

Managing a complex cyber investigation is not just about managing digital evidence acquisition. This course comprises three modules: 1 - the problem; 2 – the profession; 3 – the processes.

MODULE 1 – The Problem

What should be investigated (cybercriminology)?

What should be investigated (strategic practice)?

MODULE 2 – The Profession

Is investigation a profession?

What ethical issues are engaged during an investigation?

How can investigation be managed ethically?

MODULE 3 – The Processes

How are risks and resources managed?

How are investigation decisions made?

What legal frameworks are engaged by investigation management?

What happens when an investigation reaches the border?

How are internal investigations managed?

Course review

2. What level is this course?

700 Level (Specialised)

Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES	GRADUATE QUALITIES
On successful completion of this course, you should be able to...	Completing these tasks successfully will contribute to you becoming...
① Demonstrate understanding of professional investigation management and professional practice	Knowledgeable Ethical
② Demonstrate in-depth knowledge of the management of securing and presenting evidence relating to cybercrime and digital data integrity breaches.	Knowledgeable
③ Critically analyse the role of digital deviancy and its investigation in society including how each might be a source of criminal and/or social harm	Creative and critical thinker
④ Use decision-making and problem-solving	Empowered Ethical
⑤ Communicate research and findings to specialist and non-specialist audiences.	Empowered

5. Am I eligible to enrol in this course?

Refer to the [USC Glossary of terms](#) for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

SEC701

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Students will be assumed to understand technology and its role in society. They will be expected to have a working knowledge of computer systems and networks.

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment during tutorials

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1a	Quiz/zes	Individual	10%	10 multiple choice questions	Week 4	Online Test (Quiz)
All	1b	Written Piece	Individual	10%	1000 words	Week 4	Online Assignment Submission with plagiarism check
All	2	Written Piece	Individual	30%	2000 words	Week 6	Online Assignment Submission with plagiarism check
All	3	Written Piece	Individual	50%	4000 written paper	Week 13	Online Assignment Submission with plagiarism check

All - Assessment Task 1a: Knowledge check quiz

GOAL:	The goal of this task is to demonstrate knowledge and understanding of basic cybercriminology concepts introduced in the opening weeks of the course.	
PRODUCT:	Quiz/zes	
FORMAT:	Quiz	
CRITERIA:	No.	Learning Outcome assessed
	1 Answer ten questions randomly selected from a pool of questions.	1

All - Assessment Task 1b: Written piece

GOAL:	The goal of this task is to demonstrate knowledge and understanding of basic cybercriminology concepts introduced in the opening weeks of the course.	
PRODUCT:	Written Piece	
FORMAT:	More information available on Blackboard Learning Management System	

CRITERIA:	No.	Learning Outcome assessed
	1 Learners will describe and explain how a theoretical model might be used to inform the work of a cyber investigations manager.	1 3 5

All - Assessment Task 2: Review of case study investigation management

GOAL:	From a set text, learners will identify investigation management issues raised and identify how such behaviours might be manifested in a cyber investigation; what risks they might pose to the investigation; and what an investigation manager might do to prevent or resolve such problems.
PRODUCT:	Written Piece
FORMAT:	Written paper
CRITERIA:	No.
	1 Measured against the rubric published for this assessment on Blackboard which will be based on the learning outcomes.

All - Assessment Task 3: Review of investigation management circumstances and needs

GOAL:	For this task you are required to review the circumstances outlined in this complex investigation case-study scenario to answer the following questions: <ul style="list-style-type: none"> • what investigation management issues arise from these circumstances; • what are the potential sources of evidence and what investigation skills, technologies, methods, and protocols should be employed to secure this evidence; and • what systemic cybersecurity problems (if any) have been disclosed by these circumstances, and how should these be addressed?
PRODUCT:	Written Piece
FORMAT:	This assessment comprises a 4,000-word written paper reviewing a case-study scenario.
CRITERIA:	No.
	1 Applies investigation management problem-solving to a case-study scenario

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

7.1. Schedule

PERIOD AND TOPIC	ACTIVITIES
n/a	<p>The planned schedule for this course comprises three modules: 1 - the problem; 2 – the profession; 3 – the processes.</p> <p>MODULE 1 – The Problem Week 1 – What should be investigated (cybercriminology)? Week 2 – What should be investigated (strategic practice)?</p> <p>MODULE 2 – The Profession Week 3 – Is investigation a profession? Assessment 1 – quiz & short answer question Week 4 – What ethical issues are engaged during an investigation? Week 5 – How can investigation be managed ethically? Week 6 – Assessment 2 – written piece</p> <p>MODULE 3 – The Processes Week 7 – How are risks and resources managed? Week 8 – How are investigation decisions made? Week 9 - What legal frameworks are engaged by investigation management? Week 10 – What happens when an investigation reaches the border? Week 11 – How are internal investigations managed? Week 12 – Course review Week 13 – Assessment 3 written piece based on investigation scenario</p>

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Blackboard site – Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

Please note that you need to have regular access to the resource(s) listed below. Resources may be required or recommended.

REQUIRED?	AUTHOR	YEAR	TITLE	PUBLISHER
Recommended	Thomas HOLT, Adam BOSSLER & Kathryn SIEGFRIED-SPELLAR	2018	Cybercrime and Digital Forensics	Routledge
Recommended	Graeme Edwards	2019	Cybercrime Investigators Handbook	John Wiley & Sons
Recommended	Peter Stelfox	2009	Criminal Investigation	Willan Pub
Recommended	Robert Moore	2010	Cybercrime	Anderson Publishing
Recommended	Brett Shavers	2013	Placing the Suspect Behind the Keyboard	Syngress Press

8.2. Specific requirements

This is an online course, therefore access to a computer and a strong and stable internet connection is essential. To participate in the synchronous online tutorial classes conducted via video conference, it will be necessary for your computer to be equipped with an in-built or peripheral webcam and microphone.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the [online induction training for students](#), and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

10.2. Assessment: Additional Requirements

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:

The final mark is in the percentage range 47% to 49.4%

The course is graded using the Standard Grading scale

You have not failed an assessment task in the course due to academic misconduct.

10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate:

- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.

- 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.

- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

10.4. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the [Learning Advisers](#) web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

10.5. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to [Student Hub](#), email studentwellbeing@usc.edu.au or call 07 5430 1226.

10.6. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, , injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, [AccessAbility Services](#) can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to [Student Hub](#), email AccessAbility@usc.edu.au or call 07 5430 2890.

10.7. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website: <http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching>

10.8. General Enquiries

In person:

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **USC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **USC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **USC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **USC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au