

Welcome to INF30020 Week 1, S2, 2022

Introduction to unit:
IS Risk & Security Management

SWINBURNE
* NE *

SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Swinburne
▶ think forward

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

CRICOS Provider: 00111D | T.OID: 3059

1



Welcome

Unit Convener and lecturer

Dr. Paul Scifleet (Lecturer & *primary contact for this Unit*)
pscifleet@swin.edu.au

- Weekly online presentations: usually available on Monday's, preceding Weds classes
- Face to Face classes/ workshops (2hrs) on campus: 8:30am, 10:30am, numbers are limited and you must go to your timetable assigned class
- Consultations: On campus on Monday or Wednesday afternoons, by MS Teams or Zoom at other times, all by appointment please

Please go to your registered classes.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

Welcome to INF30020



In this unit, you will be introduced to **information risk and security management** as it applies to **contemporary organisations**. We will be examining the **knowledge and techniques** organisations apply to assessing the risks to their information assets and in so doing, how they provide for improved information security. You will learn about information risk and security management through **real-world case-based scenarios** and become familiar with approaches to **information governance and assurance**.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

This weeks learning plan



1. Familiarise yourself the structure of the Unit of Study including,
 - Learning activities, assessment items
 - Class approach and engagement
2. Begin to engage with unit content: Canvas, pre-recorded online lecture, face to face classes and readings
3. Your aim in week 1 is to develop a conceptual understanding of *Information Systems risk and security management* in a global business context and to establish a working knowledge of some key concepts
 - Information Systems Security *and what is at risk* (the information assets of an organisation)
 - Foundation concepts, key characteristics (listed on the final slide)
 - Read, *Whitman, Chapter 1*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Summary, schedule and assessment

SWIN
BUR
NE

Slide 5

| Week | Week Beginning | Weekly Teaching and Learning | Assessment and Learning activities |
|--|----------------|---|--|
| 1 | 01 August | Introduction and Overview: IS risk and security | Class activity & reading (TBA) |
| 2 | 08 August | Information Security & risks I | Class activity & reading (TBA); Submit CLA #1, Friday 11 August |
| 3 | 15 August | Information Security & risks II | Class activity & reading (TBA) |
| 4 | 22 August | Assessing security and establishing Internal Control | Class activity & reading (TBA); Submit CLA #2, Friday 26 August |
| 5 | 29 August | Mitigation, treatment & control I | Class activity & reading (TBA) |
| 6 | 05 September | Mitigation, treatment & control II | Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September |
| Mid Semester Break – 12 September to 18 September. ISRS Report Part A, due Friday 16 September. | | | |
| 7 | 19 September | Information Security & Information Governance | Group Warm-up (TBA); Submit in class, Wednesday 21 September |
| 8 | 26 September | Business Continuity Management | Class activity & reading (TBA); |
| 9 | 03 October | Contingency Planning | Class activity & reading (TBA); Submit CLA #3, Friday 07 October |
| 10 | 10 October | Cybersecurity and Business Continuity Management | Class activity & reading (TBA); |
| 11 | 17 October | Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring | Class activity & reading (TBA); Submit Report Part B, Friday 21 October |
| 12 | 24 October | Information Security ethics & compliance and pre-quiz revision | Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October |

Classes

- 1x 40- min pre-recorded lecture posted Monday mornings for review prior to upcoming Weds
- Week 1, introduction pre class
- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30

Assessments

- Continuous learning activities (3 total)
- Individual & group (major) assignment expected release dates at end of week 2 and week 6
- 2 Class quizzes

News

- Guest presentations
 - Program to be confirmed
- ISACA student group
- *All parts of unit of study are relevant to you learning and assessment*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5

Unit administration

SWIN
BUR
NE

Slide 6

Schedule and assessment

| Types | Individual or Group task | Weighting | Assessment ULOs |
|--|--|-----------|-----------------|
| Risk and security management report (part A) | Individual Due: 11:59pm, Friday 16 September | 25% | 1, 2, 3, 5 |
| Risk and security management report (part B) | Group Due: 11:59pm, Friday 21 October; Warm up exercise Weds 21 September. | 25% | 2, 3, 4, 5 |
| Continuous Learning Activities | Individual (Fridays ¹ at 5:30pm set set weeks, see Canvas schedule) | 30% | 3, 4, 5 |
| Quizzes (Online) | Individual (6 th & 12 th week) | 20% | 1 3, 4 |

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

6

Swinburne



Student Group

Business IT meets security!



If you are interested in

- Student community leadership
- Developing a professional career in Information security management and cybersecurity
- Professional career networking
- Being part of the international community of ISACA student chapters

Get in touch and participate

How to Join
Like and Join through our Facebook Page!
 @swininfosec or "Swinburne Information Security Society"



7

Unit administration

Managing communications and expectations

1. Unit Communication, through classes, canvas, announcements and discussion forums, email, MS Teams or Zoom consultations
 - Only your student account OR Canvas in-system/ clear subject
2. Realistic expectations:
 - Professional and courteous and friendly conduct with peers, colleagues and staff throughout the study period
 - *Engage, participate (when you can) in class and group discussions*
 - *Complete weekly required readings and self-directed learning activities*
 - Raise issues with me as they arise, I always aim to respond expeditiously and compassionately
 - Delivery of high-quality, not-plagiarised, not involving cheating work
3. Unrealistic expectations
 - Answering your emails after 5:30pm weekdays and on weekends
 - Requests for last minute extensions (without cause)

SWINBURNE

Slide 8

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8

Unit administration



Referencing and plagiarism: *the rules apply*

1. Referencing is crucial in any university-level assignments
 - Swinburne Harvard Style is required for assignments in this unit
 - See 'Harvard Style Guide' PDF in Resources Folder on Blackboard
2. Know the difference between a Reference List and a Bibliography
 - A Reference List is a list of all the information sources you cite in your work
 - A Bibliography is a list of all the information sources you cite in your work PLUS other sources you have looked at while preparing your work but did not actually use.
 - In this unit you will be asked to produce reference lists for your assignments
3. Please refer to university policy regarding referencing and plagiarism
 - If you are not sure AND/OR want to improve your referencing skills AND/OR want to avoid plagiarism, please ask our librarians

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

9

Unit readings



Required textbook & readings

1. During the semester students are required to familiarise themselves with
 - a. relevant Information Security standards for this area of study, including the AGs Protective Security Policy Framework, Australian Government Information Security Manual, *AS/NZS ISO/IEC 27005:2012 : Information technology - Security techniques - Information security risk management*
 - b. relevant Risk Management standards and guidelines for this area of study ISO/IEC 13335; **NIST SP 800-30; AS/NZS ISO 31000:2018; HB 254-2005** : Governance, risk management, control and assurance (e.g. ISS 1)



Recommended introductory reading for week 1 (e-book through library)

Whitman, Michael E. and Mattord, Herbert J.
Management of information security. Sixth Edition.,
 Stamford, Conn. : Cengage Learning, 2018,
Chapter 1

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

10

Australian Signals Directorate The Australian Cyber Security Centre

Australian Government Information Security Manual



Slide 11

The Australian Government Information Security Manual (ISM) represents the considered advice of the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under section 7(1)(ca) of the *Intelligence Services Act 2001*.


The (ISM) outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals and information technology managers.



INNOVATION | BUSINESS | DESIGN
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11

Continuous learning activities



Slide 12

Continuous learning activities (Individual CLAs 30% of marks)

- Are of two types
 - A. CLA#1-3 written submissions 10 marks each
 - B. **Face to Face class activities**

F2F Activities: F2F classes each week will involve exercises designed to review all unit content and undertake activities that feed directly into your required learning for assessment tasks.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN
12

12

Weekly learning activities



Weekly learning activities (Individual CLAs 30% of marks)

- Are of two types
 - A. **CLA#1-3 witten submissions 10 marks each**
 - B. Face to Face class activities

CLA activities: A 1 page submission *in Canvas at set weeks* from week 1 - week 12. There are 3 CLAs, worth 10 marks each, requiring you to answer questions asked about a reading correctly, to demonstration your knowledge with some limited synthesis and some limited analysis involved

CLA#1 is due Friday 12 August

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13

13

Continuous Learning Activities



How to approach your CLAs

- For each activity, you will be asked to respond to between 1- 4 questions
- Prepare between a half to 1-page written response to the questions identifying key points that answer the question asked
- Marks will be awarded for clear concise answers to the questions asked that demonstrate:
 - Thought, reflection and evaluation in context of the question asked unit learning
 - Draw on relevant unit materials
 - Well-focused and avoiding vague generalisations
- Questions cannot be answered with a simple yes or no but must demonstrate your connection with unit contents
- Marks awarded are based on your answer and your written response

14

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14

Wednesday's classes 8:30 am and 10:30am



Why not call this unit.... Cybersecurity?

Information Security
(InfoSec): the protection of
information assets, whether
in storage processing or
transmission, via the
application of policy &
procedures, education,
training & awareness, and
technology *Assets and
processes*

1. Read Whitman, Chapter 1
2. Undertake a quick
Internet search, *identify a
recent data breach* (last 6
months), take brief notes
3. Review CLA#1 in
preparation

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

15

15

Thank you

Questions

Terms for week 1)

1. Information Systems *Risk* and *Security* ...
importance of internal control , an
InfoSec definition of risk
2. The CIA (*Confidentiality, Integrity,
Availability*)
3. Other key terms from week 1: *Infosec,
data breach, threat, vulnerability,
malware*

Swinburne
▶ think *forward*

SWIN
BUR
NE

SWINBURNE
UNIVERSITY OF
TECHNOLOGY

16