UNIVERSITY OF CANBERRA

Information Security

Unit code and version	11759.1
Unit offering option	216989
Study level	Level 3 - Undergraduate Advanced Unit
Credit points	3
Faculty	Faculty of Science and Technology
Discipline	Academic Program Area - Technology
Unit offering details	Semester 1, 2024 , ON-CAMPUS , UC - Canberra, Bruce
Unit convener name and contact details	Dr Abu Barkat ullah (Barkat) Phone No: (02) 6201 5044 Email: Abu.Barkatullah@canberra.edu.au
Administrative contact details	Student Central Building 1, Level B Email: Student.Centre@canberra.edu.au Phone: 1300 301 727

Academic content

Unit description

This unit examines the information security threats and vulnerabilities of IT-based information systems. A risk management approach is used to develop an understanding of the policies, practices and technologies needed to provide for an appropriate level of security. Information security policy is considered and the various security needs, from managerial to technical, are examined in the context of current and future information systems. This unit may be cotaught with 6682 Information Security PG.

Learning outcomes

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

1. Interpret and integrate organisational security practices;
2. Analyse information security risks in personal and organisational situations and prepare appropriate reports for specific and non-specific audiences; and
3. Synthesise knowledge and skills to design information security requirements.

Graduate attributes

1. UC graduates are professional
    - communicate effectively
    - display initiative and drive, and use their organisation skills to plan and manage their workload
    - employ up-to-date and relevant knowledge and skills
    - take pride in their professional and personal integrity
    - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
2. UC graduates are global citizens
    - behave ethically and sustainably in their professional and personal lives
    - make creative use of technology in their learning and professional lives
3. UC graduates are lifelong learners
    - adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas
    - evaluate and adopt new technology
    - reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development

Skills development

As students of the University of Canberra, you will develop your critical thinking skills, your ability to solve complex problems, your ability to work with others, your confidence to learn independently, your written communication skills, your spoken communication skills and a number of work-related knowledge and skills.

Prerequisites

Must have passed 39 credit points including 11486 Systems Analysis and Modelling.

Corequisites

None.

This unit is part of courses accredited by the Australian Computer Society. It meets the following skill categories

ACS Accreditation

This unit is part of courses accredited by the Australian Computer Society (ACS)

Skills Framework for the Information Age (SFIA) v8

This unit meets the following SFIA skills specifications:
Information security SCTY
Security operations SCAD

SFIA skills are defined by levels of responsibility based on autonomy, influence, complexity, business skills, and knowledge. Although this unit may cover knowledge and skills at higher levels, it is expected that graduates of undergraduate degrees will be capable of operating at Level 2 overall.

Seoul Accord
The UC generic attributes address most of the requirements of the Seoul Accord. The remaining skills that are addressed in this unit are:
2. Knowledge for Solving Computing Problems
3. Problem Analysis
4. Design/Development of Solutions

5. Modern tool usage

This unit addresses a complex computing problem that has the following characteristics:

- involves wide-ranging or conflicting technical, computing, and other issues;
- has no obvious solution, and requires conceptual thinking and innovative analysis to formulate suitable abstract models;
- a solution requires the use of in-depth computing or domain knowledge and an analytical approach that is based on well-founded principles;
- involves infrequently encountered issues;
- is outside problems encompassed by standards and standard practice for professional computing;
- involves diverse groups of stakeholders with widely varying needs;
- has significant consequences in a range of contexts;
- is a high-level problem possibly including many component parts or sub-problems;
- identification of a requirement or the cause of a problem is ill defined or unknown.

These complex computing problems are assessed in the following assessment items:

- Security evaluation assessment
- Final Assessment

This unit is co-taught with 6682 Information Security PG

Timetable of activities

Week	Class Topics	Tutorials / Due Dates
1	Introduction to Information Security	There is no tutorial in Week 1
2	Information Security Overview: • Risk Management and Controls • Security Models • Management Consideration • Information Assets	Tutorial work and online discussions
3	Information Security Policy	Tutorial work and online discussions
4	ISO 27000 Series, CoBIT, ITIL	Tutorial work and online discussions
5	Risk Management and Risk Assessment	Tutorial work and online discussions

6	Protection Mechanisms	Tutorial work and online discussions
7	Information systems security development methods	Tutorial work and online discussions
8	Mid semester non-teaching week	
9	Insider threats	Tutorial work and online discussions
10	Planning contingencies	
11	Cyber Security	Tutorial work and online discussions Security Evaluation Assessment
12	Personnel Issues	Tutorial work and online discussions
13	Unit Review	Tutorial work and online discussions
14		Final Assessment

*Schedule is provisional and subject to change (via Canvas announcement)

Unit resources

Required texts

There is no required textbook for Information Security.

The following books are set as recommended readings:

- ISACA (2019), COBIT 2019, ISACA https://www.isaca.org/cobit/pages/default.aspx
- ISO27000 series – Information technology — Security techniques — Information security management systems
- Whitman, ME & Mattord, HJ (2019), Management of information security, 6th edn, Cengage Learning
- Awad, A & Fairhurst, M. (2018), Information Security : Foundations, Technologies and Applications, Institution of Engineering & Technology

- Chopra, A & Chaudhary (2019) Implementing an Information Security Management System : Security Management Based on ISO 27001 Guidelines, Apress L. P.
- Vacca, J and Vacca, J (2013) Computer and Information Security Handbook, Elsevier Science & Technology
- Chapple, M (2021), CISM Certified Information Security Manager Study Guide.John Wiley & Sons

A range of academic articles relating to Information Security will also be used to support the teaching of this unit.

Materials and equipment

None

Unit website

Each unit you are enrolled in has an online teaching site in the learning management system UCLearn. You access UCLearn through MyUC.

Assessment

Assessment item details

Security evaluation assessment

Due date

Week 11 Friday 11:59 PM

Weighting

30%

Assessment details

This is an individual assignment and will involve students conducting a security evaluation of their personal ICT use and reporting on the results of this evaluation. Students will be expected to make detailed recommendations for the improvement of their personal situation. Further details will be provided on the unit website.

Addresses learning outcomes

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

- 1. Interpret and integrate organisational security practices;
- 2. Analyse information security risks in personal and organisational situations and prepare appropriate reports for specific and non-specific audiences; and
- 3. Synthesise knowledge and skills to design information security requirements.

Related graduate attributes

1. UC graduates are professional
    - communicate effectively
    - display initiative and drive, and use their organisation skills to plan and manage their workload
    - employ up-to-date and relevant knowledge and skills
    - take pride in their professional and personal integrity
    - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
2. UC graduates are global citizens
    - behave ethically and sustainably in their professional and personal lives

    - make creative use of technology in their learning and professional lives
3. UC graduates are lifelong learners
    - adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas
    - reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development

Tutorial work and online discussions

Due date

During semester and in classes

Weighting

30%

Assessment details

Preparation and discussion of unit material, along with tutorial based presentations are an important component of this unit. Students are encouraged to prepare for tutorials and engage fully in discussions during tutorials. Part of this preparation will involve a one to two page summary of the relevant issues for the tutorial and students will be required to submit these notes during the semester prior to the relevant tutorial. The tutor will provide an assessment for each student based on their participation in discussions and how well they prepare for the tutorials. This assessment item will also involve contributions to online discussions on information security issues. Note that participation involves more than just attendance.

Addresses learning outcomes

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

- 1. Interpret and integrate organisational security practices;
- 2. Analyse information security risks in personal and organisational situations and prepare appropriate reports for specific and non-specific audiences; and
- 3. Synthesise knowledge and skills to design information security requirements.

Related graduate attributes

1. UC graduates are professional
    - communicate effectively
    - display initiative and drive, and use their organisation skills to plan and manage their workload
    - employ up-to-date and relevant knowledge and skills
    - take pride in their professional and personal integrity
    - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
2. UC graduates are global citizens
    - behave ethically and sustainably in their professional and personal lives
3. UC graduates are lifelong learners
    - adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas
    - reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development

Final Assessment

Due date

Week 14, 12:00 PM on Wednesday, 8 May 2024

Weighting

40%

Assessment details

The final assessment will be a 48-hour open-book assessment. The assessment will open at 12:00 PM on Monday, 6 May 2024, and close at 12:00 PM on Wednesday, 8 May 2024.
A mark of 50% or greater in this assessment is required to pass the unit.

Addresses learning outcomes

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

- 1. Interpret and integrate organisational security practices;
- 2. Analyse information security risks in personal and organisational situations and prepare appropriate reports for specific and non-specific audiences; and
- 3. Synthesise knowledge and skills to design information security requirements.

Related graduate attributes

1. UC graduates are professional
   - communicate effectively
   - display initiative and drive, and use their organisation skills to plan and manage their workload
   - employ up-to-date and relevant knowledge and skills
   - take pride in their professional and personal integrity
   - use creativity, critical thinking, analysis and research skills to solve theoretical and real-world problems
3. UC graduates are lifelong learners
   - adapt to complexity, ambiguity and change by being flexible and keen to engage with new ideas
   - reflect on their own practice, updating and adapting their knowledge and skills for continual professional and academic development

Submission of assessment items

Students should keep a copy of all assessment items that are submitted at least until unit grades have been published at the end of semester.

Extensions

Students can apply for an extension to the submission due date for an assessment item due to extenuating, evidenced circumstances (specific details are found in the Assessment Procedures). An extension must be applied for before the due date. Documentary evidence (e.g. medical certificate) will be expected for an extension to be granted, however this will not guarantee that the application will be successful. The Unit Convener or relevant Program Director/Course Convener will decide whether to grant an extension and the length of the extension.

An Assignment Extension form is available from the Student Forms page.

Late submissions

The following late submission period and penalty is applicable to any teaching period commencing after 1 April 2024.

To support the provision of timely feedback to students within the unit, late penalties will apply for summative assessments where late submission is permitted. Late submissions without an approved extension or reasonable adjustment will result in a penalty of a mark reduction of 10% of the maximum available marks for the assessment item per day (or part thereof) up to and including three calendar days. If a student submits more than three calendar days late without an approved extension or reasonable adjustment, the student will be allocated a mark of zero for that assessment, with no feedback provided.

Approval of extensions based on extenuating circumstances will be dependent upon the production of supporting documentation and at the discretion of the unit convener.

For teaching periods commencing prior to 1 April 2024, a late penalty of 5 % of the maximum available marks for the assessment item per day (or part thereof) was applied up to and including seven calendar days. An assignment submitted over 7 days late will not be accepted.

Special assessment requirements

In order to pass this unit, students have to obtain total marks of 50% or greater. Some scaling of marks and academic judgement may be applied to determine students' final grades - in this process no student will be disadvantaged.In the case of any assignment that places you in jeopardy of a Fail in the whole unit, appropriate moderation procedures will be used.If there is any doubt with regard to the requirements of any particular assignments or assessment procedure, the onus for clarifying the issue rests with the student, who should contact the unit convener about the matter.

All work quoted from any source should be appropriately referenced using the “Harvard (2021)” referencing style as described in the link below (note that there is multiple versions of the Harvard referencing style, and you should use the one described here).

http://canberra.libguides.com/referencing

Students who are not familiar with referencing academic work should undertake the Academic Integrity Module.

The unit convenor reserves the right to question students on any of their submitted work for moderation and academic integrity purposes, which may result in an adjustment to the marks awarded for a specific task.

Supplementary assessment

Refer to the Assessment Policy and Assessment Procedures

Academic integrity

Students have a responsibility to uphold University standards on ethical scholarship. Good scholarship involves building on the work of others and use of others' work must be acknowledged with proper attribution made. Cheating, plagiarism, and falsification of data are dishonest practices that contravene academic values. Refer to the University's Student Charter for more information.

To enhance understanding of academic integrity, all students are expected to complete the Academic Integrity Module (AIM) at least once during their course of study. You can access this module within UCLearn (Canvas) through the 'Academic Integrity and Avoiding Plagiarism' link in the Study Help site.

Use of Text-Matching Software

The University of Canberra uses text-matching software to help students and staff reduce plagiarism and improve understanding of academic integrity. The software matches submitted text in student assignments against material from various sources: the internet, published books and journals, and previously submitted student texts.

Student responsibility

Learner engagement

Activities	Hours
Weekly lecture: 2 hours per week, 12 weeks	24

Weekly Tutorial: 1 hour per week, 11 weeks	11
Preparation for tutorial work and other general reading: 3 hours per week, 11 weeks	33
Tutorial work and online discussions	22
Security evaluation Assessment	40
Final Assessment	20
Total	150

Inclusion and engagement

It is strongly recommended that students who need assistance in undertaking the unit because of disability or an ongoing health condition register with the Inclusion and Engagement Office as soon as possible so that reasonable adjustment arrangements can be made.

Participation requirements

Attendance at classes is not compulsory but it is advisable for students to attend as many classes as possible. Students should also be aware that the subject will be examined on material covered in classes, including lectures and tutorials and it is the individual student's responsibility to ensure that they are sufficiently familiar with this material. Attendance at classes is one of the best ways of ensuring this familiarity. Do not make the mistake of assuming that the materials provided online perfectly substitute for class attendance.

Announcements are made throughout the unit, typically to clarify requirements for assignments. Any such announcements will be made using your student email account and/or placed on the unit web site. Such announcements are deemed, within two working days, to be made to the whole group. Announcements made at an organised session are deemed to be made to the whole group.

Withdrawal

If you are planning to withdraw please discuss with your Unit Convener. UC College students must also seek advice from the College.

Required IT skills

Information Security is an advanced level unit and it is generally expected that students will have a fair degree of sophistication in their knowledge of IT related matters. Students should also possess the ability to use a word processor for the production of assignments and various on-line searching tools from the Internet and the library to undertake various assignments in the unit.

Work integrated learning

None

Student feedback

All students enrolled in this unit will have opportunities to provide anonymous feedback on the unit through the InterFace Student Experience Questionnaire (ISEQ). The request for your feedback will be posted on your InterFace page at least twice during a teaching period. InterFace can be accessed through MyUC.

Changes to unit based on student feedback

Revision, update, and improvement of contents and assessments are undertaken based on students' feedback.

Authority of this unit outline

This unit outline must be read in conjunction with the University of Canberra's Policies and Procedures, including the Assessment Policy and associated Procedure. The Assessment Policy and Assessment Procedure include information on matters such as plagiarism, grade descriptors, moderation, feedback, and deferred exams.

Any change to the information contained in the Academic content and Assessment sections of this document, will only be made by the Unit

Convener if the written agreement of the Program Director and a majority of students has been obtained; and if written advice of the change is then provided on the teaching site in UCLearn. If this is not possible, written advice of the change must be then forwarded to each student enrolled in the unit at their registered term address. Any individual student who believes themselves to be disadvantaged by a change is encouraged to discuss the matter with the Unit Convener.

Authority Text

Main

> Exception – Potential changes to a unit's learning activities and assessment items (Approved Academic Board 2020)
>
> In the event of Australian Government and/or ACT Government directive, such as those requiring physical distancing and restrictions on movement because of a pandemic, learning activities and/or assessment items in some units may change. These changes will not be updated in the published Unit Outline but will be communicated to students via the unit’s UCLearn (Canvas) teaching site. The new learning activities and/or assessment items will continue to meet the unit's learning outcomes, as described in the Unit Outline.
>
> New learning activities and/or assessment items will be available on the unit's UCLearn (Canvas) teaching site. Please contact the Unit Convener with any questions.

University of Canberra, Bruce ACT 2617 Australia

+61 2 6201 5111

ABN 81 633 873 422

CRICOS 00212K

TEQSA Provider ID: PRV12003 (Australian University)

UC acknowledges the Ngunnawal people, traditional custodians of the lands where Bruce campus is situated. We wish to acknowledge and respect their continuing culture and the contribution they make to the life of Canberra and the region. We also acknowledge all other First Nations Peoples on whose lands we gather.