UNSW Course Outline

ZEIT8021 Information Assurance and Security - 2024

Published on the 09 Feb 2024

General Course Information

Course Code : ZEIT8021
Year : 2024
Term : Semester 1
Teaching Period : Z1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

The ZEIT 8021 Information Assurance and Security course is one of the core courses for the Masters in Cybersecurity. It is a standard postgraduate course, available only through distance delivery mode, worth six Units of Credit (6 UOC) and requires approximately 160 hrs of student study time. **No prerequisites are required**. This course aims to lay a firm foundation for cybersecurity knowledge, providing the ability for students from many related fields to gain perspective of modern cybersecurity threats and corresponding defensive controls and explore effective computer security and risk management strategies with particular emphasis on Information Assurance (IA) practices and techniques.

Within the course, IA practices and techniques refer to the steps involved in protecting information systems as part of the enterprise. Three common terms are associated with the definition of information assurance: **confidentiality**, **integrity**, and **availability**. While IA is a field in and of itself, it can be thought of as logically occupying a position between Information Technology (IT), Software and Systems Engineering, and Security. Information Assurance can be thought of as ensuring that systems maintain these three qualities of the system.

IA involves keeping information **confidential**. This means that only those authorised to view information can access it. For example, information is classified or categorised within the military so that only people with certain clearance levels are allowed access to confidential information. Civilian organisations also categorise data, respecting the impact of loss or misuse.

Integrity involves ensuring that data and information systems may be changed by authorised people for authorised purposes. IA may be used to take steps to maintain integrity, such as having anti-malware software in place so that data will not be altered or destroyed and having policies in place so that users know how to properly utilise their systems to minimise the effect of (internal) user error, or (external) malicious code.

In the context of IA, **availability** is the ability of a system to be available for use by those who are allowed to access it. Protecting the availability can involve protecting against malicious code, hackers and any other threat that could block access to the information system or an explicit denial of service attack.

This master level 6.0 unit course is designed with the tools to integrate and apply IA knowledge to the system phases of System Development, System Acquisition, System Operation and Service Delivery. Along the way, we will review the process of considering Information Assurance from requirements elicitation through system delivery and operation to system disposal.

This course is theoretical and covers not only the very broad content of the ISC2 CISSP® certification but also draws on the CMMI for Development and for Services frameworks to provide a holistic application of Information Assurance considerations. It draws on ISC2 material as well as other scholarly sources.

Course Aims

This course aims to:

To provide students with a deep understanding of the technical, management and organisational aspects of Information Assurance within a holistic legal and social framework.

Course Learning Outcomes

Course Learning Outcomes	Australian Computing Society (ACS)
CLO1 : Make a realistic assessment of information assurance issues through system lifecycle phases	• ACS1 : Institutional Commitment to ICT education
CLO2 : Be able to use risk-based and compliance-based strategies to identify security requirements	• ACS1 : Institutional Commitment to ICT education
CLO3 : Be aware of technologies that can be used to translate security requirements into system design and implementation elements	• ACS1 : Institutional Commitment to ICT education • ACS3 : Technological Resources for ICT Education
CLO4 : Show an understanding of different types of engineering and compliance testing required for information assurance related functionality	• ACS1 : Institutional Commitment to ICT education • ACS2 : ICT Academic Leadership and Staffing
CLO5 : Demonstrate an understanding of integrated risk-based best practices within systems that must deliver a level of information assurance	• ACS3 : Technological Resources for ICT Education
CLO6 : Demonstrate an understanding of security in steady state operations and management of secure systems	• ACS4 : Monitoring, Review and Improvement

Course Learning Outcomes	Assessment Item
CLO1 : Make a realistic assessment of information assurance issues through system lifecycle phases	• Assignment 1 - Business Case • Assignment 2 - Threat Analysis • Assignment 3 - Reflective Article
CLO2 : Be able to use risk-based and compliance-based strategies to identify security requirements	• Assignment 2 - Threat Analysis
CLO3 : Be aware of technologies that can be used to translate security requirements into system design and implementation elements	• Assignment 3 - Reflective Article
CLO4 : Show an understanding of different types of engineering and compliance testing required for information assurance related functionality	
CLO5 : Demonstrate an understanding of integrated risk-based best practices within systems that must deliver a level of information assurance	• Assignment 2 - Threat Analysis
CLO6 : Demonstrate an understanding of security in steady state operations and management of secure systems	• Assignment 3 - Reflective Article • Assignment 2 - Threat Analysis

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Australian Computing Society (ACS)
Assignment 1 - Business Case Assessment Format: Individual	10%	Due Date: 04/03/2024 11:55 PM	• ACS1 : Institutional Commitment to ICT education • ACS4 : Monitoring, Review and Improvement
Assignment 2 - Threat Analysis Assessment Format: Group	30%	Due Date: 02/04/2024 11:55 PM	• ACS2 : ICT Academic Leadership and Staffing
Assignment 3 - Reflective Article Assessment Format: Individual	20%	Due Date: 06/05/2024 11:55 PM	• ACS1 : Institutional Commitment to ICT education • ACS3 : Technological Resources for ICT Education
Assignment 4 - Security Plan Assessment Format: Individual	40%	Due Date: 03/06/2024 11:55 PM	• ACS1 : Institutional Commitment to ICT education • ACS2 : ICT Academic Leadership and Staffing • ACS3 : Technological Resources for ICT Education • ACS4 : Monitoring, Review and Improvement

Assessment Details

Assignment 1 - Business Case

Assessment Overview

The first assessment addresses the need for an effective information assurance program. It is an individual effort.

Course Learning Outcomes

- CLO1 : Make a realistic assessment of information assurance issues through system lifecycle phases

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Assignment 2 - Threat Analysis

Assessment Overview

This is to be completed in a group of 2 or 3 to analyse the threat associated with a particular system. It will assess student’s ability to work together on a topic and research additional sources.

Course Learning Outcomes

- CLO1 : Make a realistic assessment of information assurance issues through system lifecycle phases
- CLO2 : Be able to use risk-based and compliance-based strategies to identify security requirements
- CLO5 : Demonstrate an understanding of integrated risk-based best practices within systems that must deliver a level of information assurance
- CLO6 : Demonstrate an understanding of security in steady state operations and management of secure systems

Assignment 3 - Reflective Article

Assessment Overview

This assessment is in two parts — a short piece analysing an event reported in the mainstream media; and a response to another student’s reflection. It will assess the student’s ability to apply topic areas to relevant contemporary issues.

Course Learning Outcomes

- CLO1 : Make a realistic assessment of information assurance issues through system lifecycle phases
- CLO3 : Be aware of technologies that can be used to translate security requirements into system design and implementation elements
- CLO6 : Demonstrate an understanding of security in steady state operations and management of secure systems

Assignment submission Turnitin type

This is not a Turnitin assignment

Assignment 4 - Security Plan

Assessment Overview

Development of the Security Plan will require deep research on a topic. Online readings (in MOODLE) plus students’ additional research will provide essential background for this assignment.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

General Assessment Information

Late Submission of Assessment

No extensions are possible without a formal request to the lecturer for special consideration prior to the due date.

Please note the policy states that work commitments are not normally considered a justification for late submission of work.

Unless prior arrangement is made with the lecturer or a formal application for special consideration is submitted, a penalty of 5% of the total available mark for the assessment will apply for each day that an assessment item is late up to a maximum of 5 days (120 hours) after which an assessment can no longer be submitted and a grade of 0 will be applied.

Penalties for late submission apply from the original submission date, unless that date is formally varied by agreement. If a late submission is allowed, the extra time granted should be viewed solely as a grace period. To be clear, should the delayed date not be met, the penalty applies from the original date of submission, not from the end of the grace period.

Grading Basis

Standard

Requirements to pass course

Assessment Criteria: Compulsory components or minimum performance standards

All three assessment items form the requirements to complete this subject. To pass this subject students will need to achieve at least 50 marks out of a total 100 marks overall.

All marks obtained for assessment items during the

session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

All assignments are to be delivered using the links in Moodle. No assignment will be accepted by other means (such as email), The criteria by which marks are assigned are described in the Assignment Grading Criteria which can be found on the Moodle site.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Lecture	Introduction to Information Assurance Groups for Assessment 2 finalised
Week 2 : 4 March - 8 March	Lecture	Security and Risk Management Assignment 1 due
Week 3 : 11 March - 15 March	Lecture	Asset Security
Week 4 : 18 March - 22 March	Lecture	Recap Assessment 1
Week 5 : 25 March - 29 March	Lecture	Security Engineering
Week 6 : 1 April - 5 April	Lecture	Security Engineering 2 Assignment 2 due
Week 7 : 22 April - 26 April	Lecture	Recap Assessment 2
Week 8 : 29 April - 3 May	Lecture	Communications and Network Security
Week 9 : 6 May - 10 May	Lecture	Identity and Access Management Assignment 3 due
Week 10 : 13 May - 17 May	Lecture	Security Assessment
Week 11 : 20 May - 24 May	Lecture	Security Operations Assignment 3 results (no recap)
Week 12 : 27 May - 31 May	Lecture	Secure Systems Delivery
Week 13 : 3 June - 7 June	Lecture	Revision Final Assessment Due

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

Each week in the course follows the same schedule.

Times are as at Canberra:

1. *Monday at 1800 the online session runs on Moodle. These sessions will be recorded for later reference;*
2. *Tuesday to Thursday lecturers are available to answer questions via email; and,*
3. *Monday any assessment due that week (in bold below) must be submitted by 23:55.*

The semester will follow the schedule below week to week.

Course Resources

Prescribed Resources

A variety of resource materials will be made available.

These comprise:

- *Extensive slides and presentation notes in the form of PowerPoint slides covering the material presented. These will be made available through the Moodle pages for this course*
- *Recommended papers and chapters from textbooks, Internet based documents and other sources. In general, these materials will be available through the Moodle pages.*

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Huadong Mo		R101, B20, UNSW Canberra	+61 2 5114 5183	Huadong is usually available by email and during online consultation times via the Moodle Collaborate platform. I also welcome face-to-face discussion in my office during working hours by email appointment.	No	Yes
Lecturer	Michael M cGarity				Michael is only available by appointment for virtual discussion, or via Blackboard discussions on Monday evenings (see Course Schedule section below).	No	No

Other Useful Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the “On-going Student Feedback” link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: [Student Code of Conduct (unsw.edu.au)]()

Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;
- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW 'fit to sit or submit' requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,
- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty, for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
- Google Chrome 50+
- Safari 10+

Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
- Windows 10,
- Mac OSX Sierra,
- iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au

Phone: (02) 9385-1333

International: +61 2 9385 1333

For all other Moodle issues please contact:

External TELT Support

Email: externalteltsupport@unsw.edu.au

Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 3pm, Mon to Fri)