UNSW Course Outline

ZZCA9206 Cyber Risk and Resilience - 2024

Published on the 28 Feb 2024

General Course Information

Course Code : ZZCA9206
Year : 2024
Term : Hexamester 2
Teaching Period : KF
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : Canberra School of Professional Studies
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra City
Campus : Canberra City
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Cyber resilience is the organisational ability to deliver business or operational outcomes despite cyber attack. True resilience is a measure of both business and cyber understanding. This course provides students with the skills necessary to manage contemporary risks through gaining a systematic understanding of the principles and policies for developing the resilience of communities, businesses, and critical systems.

Course Aims

To develop skilled professionals who can use risk assessment to forward their cyber understanding, and to positively affect business and professions.

Relationship to Other Courses

ZZEN9201 Foundations of Cyber Security is a pre-requisite.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.
CLO2 : Analyse and develop a cyber risk profile for an organisation or project.
CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment approaches, and when it is appropriate to use them.
CLO4 : Develop appropriate risk assessments and recommendations.
CLO5 : Communicate the results of risk assessments effectively to key stakeholders.
CLO6 : Integrate cyber resilience frameworks into business needs.

Course Learning Outcomes	Assessment Item
CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.	• Weekly quizzes • Case study and presentation • Reflective essay • Risk assessment consulting report
CLO2 : Analyse and develop a cyber risk profile for an organisation or project.	• Weekly quizzes • Risk assessment consulting report
CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment approaches, and when it is appropriate to use them.	• Case study and presentation • Reflective essay • Weekly quizzes • Risk assessment consulting report
CLO4 : Develop appropriate risk assessments and recommendations.	• Weekly quizzes • Risk assessment consulting report
CLO5 : Communicate the results of risk assessments effectively to key stakeholders.	• Case study and presentation • Reflective essay • Weekly quizzes • Risk assessment consulting report
CLO6 : Integrate cyber resilience frameworks into business needs.	• Weekly quizzes • Risk assessment consulting report

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

Learning and Teaching in this course

The Learning 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.

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

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Weekly quizzes Assessment Format: Individual	25%	Due Date: Week 2 - 6
Case study and presentation Assessment Format: Individual	25%	Due Date: Sunday Week 4
Reflective essay Assessment Format: Individual	10%	Due Date: Sunday Week 5
Risk assessment consulting report Assessment Format: Individual	40%	Due Date: Monday Week 7

Assessment Details

Weekly quizzes

Assessment Overview

A brief quiz held at the end of each weeks content.

Course Learning Outcomes

- CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.
- CLO2 : Analyse and develop a cyber risk profile for an organisation or project.
- CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment approaches, and when it is appropriate to use them.
- CLO4 : Develop appropriate risk assessments and recommendations.
- CLO5 : Communicate the results of risk assessments effectively to key stakeholders.
- CLO6 : Integrate cyber resilience frameworks into business needs.

Assessment Length

1 hour

Case study and presentation

Assessment Overview

Students will prepare a brief presentation that explore a case study related to risk monitoring practise in a provided case study.

Course Learning Outcomes

- CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.
- CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment

approaches, and when it is appropriate to use them.
- CLO5 : Communicate the results of risk assessments effectively to key stakeholders.

Assessment Length

10 minutes

Reflective essay

Assessment Overview

This reflective essay focuses on understanding the differences between qualitative and quantitative risk assessment methods.

Course Learning Outcomes

- CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.
- CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment approaches, and when it is appropriate to use them.
- CLO5 : Communicate the results of risk assessments effectively to key stakeholders.

Assessment Length

600 - 800 words

Risk assessment consulting report

Assessment Overview

Students will provide a report that addresses key assets, a risk assessment and a business impact analysis.

Course Learning Outcomes

- CLO1 : Apply current risk assessment best-practice and standards, and effectively apply them to new situations.
- CLO2 : Analyse and develop a cyber risk profile for an organisation or project.
- CLO3 : Explain different forms of risk, strengths and limitations of a range of risk assessment approaches, and when it is appropriate to use them.
- CLO4 : Develop appropriate risk assessments and recommendations.
- CLO5 : Communicate the results of risk assessments effectively to key stakeholders.
- CLO6 : Integrate cyber resilience frameworks into business needs.

Assessment Length

2,500 words

General Assessment Information

Generative AI Statement:

UNSW accepts the potential of these tools and is excited to explore ways to use Generative AI (GenAI) to enrich your learning experience while maintaining the integrity of our programs and, therefore, of your degrees. We expect that, as we learn about how best to do this, our policies will adapt. For advice and guidance on how to use GenAI please see the Generative AI Statement in Moodle, or refer to the Universities resources: Chat GPT & Generative AI at UNSW | UNSW Current Students.

There are three key principles across the university:

1. Always do what you are asked to do in the assessment; if you don't follow the instructions, you can't get marks.
2. If you are asked to do your own work, then that is what you should do, as we want to see that *you* have undertaken that learning rather than someone or something else.
3. When you incorporate ideas that are not your own, you should always acknowledge them. That applies in the world of AI, just as it did before.

In ***this course,*** the permitted level of GenAI use is '***Drafting Assistance***'.

What is Drafting Assistance?

As this course's assessment tasks involve some planning or creative processes, you are permitted to use software to generate initial drafts, ideas, structures, etc. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the software should not be a part of your final submission. It is a good idea to keep copies of your initial drafts to show your lecturer if there is any uncertainty about the originality of your work.

Please note that your submission will be passed through an AI-text detection tool. If your marker has concerns that your answer contains passages of AI-generated text that have not been sufficiently modified, you may be asked to explain your work, but we recognise that you are permitted to use AI-generated text as a starting point, and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission, you may be referred to the UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Assessment Tolerances:

Assessment submissions have a tolerance of +/- 10% for length, meaning your submission length can go over or under the word or time limit by 10%. For example:

- A written assessment that has a 1,000-word limit can be between 900 and 1,100 words without penalty.
- An audio or video assessment that has a 10-minute time limit can be between 9 and 11 minutes without penalty.

Grading Basis

Standard

Requirements to pass course

In order to pass the course you must achieve an overall mark of at least 50%.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 11 March - 17 March	Online Activity	Overview of risk management and governance
Week 2 : 18 March - 24 March	Online Activity	The business perspective – Cyber management
Week 3 : 25 March - 31 March	Online Activity	Risk reporting, monitoring and metrics
Week 4 : 1 April - 7 April	Online Activity	Supply chain risk and resilience
Week 5 : 8 April - 14 April	Online Activity	Cyber resilience and contingency planning
Week 6 : 15 April - 21 April	Online Activity	Cyber risk and resilience in the digital age

Attendance Requirements

Not Applicable - as no class attendance is required

Course Resources

Prescribed Resources

All resources required to complete this course are available via Moodle.

Recommended Resources

Student have access to a number of additional support resources.

Please check your Moodle page for additional readings and advice relevant to the course.

Course Evaluation and Development

Evaluation and Development

Toward the end of the hexamester you will be asked to give feedback about the course, via UNSW’s MyExperience survey. Your feedback will be used, along with feedback from other stakeholders, to help improve the course. You can also contact your Course Convenor any time you have suggestions or other feedback.

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

Quality Assurance

UNSW actively monitors student learning and quality of the student experience in its programs. A random selection of completed assessment tasks may be used for quality assurance, such as determining the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of programs. All material used for such processes will be treated as confidential.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Marwa Keshk					No	Yes
Postgraduate coordinator	Tom Townsend					No	No
Lecturer	Nickolaos Koroniotis					No	No