



UNSW Course Outline

ZZCA9221 Cyber Management and Governance - 2024

Published on the 16 Jun 2024

General Course Information

Course Code : ZZCA9221

Year : 2024

Term : Hexamester 4

Teaching Period : KN

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 Management and Governance equips you with the skills for weighing competing challenges for the management of cyber and related governance activities in an organisational context. You will learn how to develop cyber strategies, policies and to apply a critical eye to the

cyber challenges facing organisations today. Building an understanding of how these governance tools impact people and the efficacy of cyber security controls and practices.

Course Aims

Cyber Management and Governance equips you with the skills for weighing competing challenges for the management of cyber and related governance activities in an organisational context. You will learn how to develop cyber strategies, policies and to apply a critical eye to the cyber challenges facing organisations today. Building an understanding of how these governance tools impact people and the efficacy of cyber security controls and practices.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Demonstrate a critical understanding of impact of cyber policy and strategy.
CLO2 : Evaluate competing risks and benefits against organisational culture.
CLO3 : Integrate emerging directions in cyber management with existing norms to shape policy and strategic organisational aims.
CLO4 : Make decisions and recommendations aligned with organisational objectives.
CLO5 : Produce executive level documentation that demonstrates ability to articulate complex concepts to non-technical audiences.

Course Learning Outcomes	Assessment Item
CLO1 : Demonstrate a critical understanding of impact of cyber policy and strategy.	<ul style="list-style-type: none">• Organisational profile• Cyber strategy• Cyber Policy Presentation
CLO2 : Evaluate competing risks and benefits against organisational culture.	<ul style="list-style-type: none">• Organisational profile• Cyber strategy• Cyber Policy Presentation
CLO3 : Integrate emerging directions in cyber management with existing norms to shape policy and strategic organisational aims.	<ul style="list-style-type: none">• Cyber strategy• Cyber Policy Presentation
CLO4 : Make decisions and recommendations aligned with organisational objectives.	<ul style="list-style-type: none">• Organisational profile• Cyber strategy• Cyber Policy Presentation
CLO5 : Produce executive level documentation that demonstrates ability to articulate complex concepts to non-technical audiences.	<ul style="list-style-type: none">• Cyber strategy• Cyber Policy Presentation

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
Organisational profile Assessment Format: Individual	25%	Due Date: Week 3
Cyber strategy Assessment Format: Individual	35%	Due Date: Week 5
Cyber Policy Presentation Assessment Format: Individual	40%	Due Date: Week 7

Assessment Details

Organisational profile

Assessment Overview

In this assessment you will develop an organisational profile that will form a foundation for the remaining assessments.

Course Learning Outcomes

- CLO1 : Demonstrate a critical understanding of impact of cyber policy and strategy.
- CLO2 : Evaluate competing risks and benefits against organisational culture.
- CLO4 : Make decisions and recommendations aligned with organisational objectives.

Assessment Length

1000 words

Assignment submission Turnitin type

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

Cyber strategy

Assessment Overview

In this assessment you will develop a Cyber Strategy for the organisation you profiled.

Course Learning Outcomes

- CLO1 : Demonstrate a critical understanding of impact of cyber policy and strategy.
- CLO2 : Evaluate competing risks and benefits against organisational culture.
- CLO3 : Integrate emerging directions in cyber management with existing norms to shape policy and strategic organisational aims.
- CLO4 : Make decisions and recommendations aligned with organisational objectives.
- CLO5 : Produce executive level documentation that demonstrates ability to articulate

complex concepts to non-technical audiences.

Assessment Length

1500 words

Assignment submission Turnitin type

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

Cyber Policy Presentation

Assessment Overview

In this assessment you will consider the policy implications of your new Cyber Strategy on the profiled organisation, highlighting and explaining the changes in policy that will be required.

Course Learning Outcomes

- CLO1 : Demonstrate a critical understanding of impact of cyber policy and strategy.
- CLO2 : Evaluate competing risks and benefits against organisational culture.
- CLO3 : Integrate emerging directions in cyber management with existing norms to shape policy and strategic organisational aims.
- CLO4 : Make decisions and recommendations aligned with organisational objectives.
- CLO5 : Produce executive level documentation that demonstrates ability to articulate complex concepts to non-technical audiences.

Assignment submission Turnitin type

Not Applicable

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.

- 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 : 1 July - 7 July	Online Activity	Cyber management and frameworks
Week 2 : 8 July - 14 July	Online Activity	Risk management and organisations
Week 3 : 15 July - 21 July	Online Activity	Cyber strategy development
Week 4 : 22 July - 28 July	Online Activity	Cyber policy development
Week 5 : 29 July - 4 August	Online Activity	Cyber leadership
Week 6 : 5 August - 11 August	Online Activity	Emerging technology and cyber

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	Tom Townsend					Yes	Yes