UNSW Course Outline

ZEIT8037 Cyber Security Risk Management - 2024

Published on the 30 Jun 2024

General Course Information

Course Code : ZEIT8037
Year : 2024
Term : Semester 2
Teaching Period : Z2
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 concept of risk is central to cyber security and developing an understanding of the exposure of the system to different threats enables security efforts to be prioritized. By determining risk and exposure, security can be managed and cost-benefit decisions can be made. This course

explores the principles and tools behind risk analysis for security, providing practical experience on a realistic case study and introduces the fundamentals of risk and risk management in a cyber security context focusing on risk, recovery and response.

Students will:

- Understand Risk Management Fundamentals
- Threats, Vulnerabilities, and Exploits
- Compliance
- Develop a Risk Management Plan
- Define various Risk Assessment Approaches
- Perform a Risk Assessment
- Identify Assets and Activities to be Protected
- Identify and Analyze Threats, Vulnerabilities, and Exploits
- Identify and Analyze Risk Mitigation Security Controls
- Planning Risk Mitigation
- Mitigate Risk with a Business Impact Analysis , Business Continuity Plan and a Computer Incident Response Team Plan.

Course Aims

This course provides an in-depth perspective on fundamental cyber security risk management principles. It examines Risk, Response, and Recovery in addition to providing a thorough overview of risk management and its implications on cyber infrastructures and compliance.

On completion the student will

- be able to understand the main issues of risk in cyber (computer and information) security;
- be able to conduct a security risk analysis, develop a plan and make cost-benefit decisions based on this;
- have an overview of how risk analysis can be used to make a business case for security.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program
CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment
CLO3 : Apply theory to implement risk mitigation security controls throughout an organisation and perform a business impact analysis
CLO4 : Undertake a computer incident response team (CIRT), a business continuity plan (BCP) and a disaster recovery plan (DRP) based on the evaluation of a risk assessment for an organisation

Course Learning Outcomes	Assessment Item
CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program	• Online Quizzes • Privacy Impact Assessment • Forum • Mini Project
CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment	• Online Quizzes • Privacy Impact Assessment • Forum • Mini Project
CLO3 : Apply theory to implement risk mitigation security controls throughout an organisation and perform a business impact analysis	• Forum • Mini Project
CLO4 : Undertake a computer incident response team (CIRT), a business continuity plan (BCP) and a disaster recovery plan (DRP) based on the evaluation of a risk assessment for an organisation	• Mini Project

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Online Quizzes Assessment Format: Individual Short Extension: Yes (3 days)	15%	Start Date: 09/08/2024 11:59 PM
Privacy Impact Assessment Assessment Format: Individual Short Extension: Yes (3 days)	15%	Start Date: Not Applicable Due Date: 26/08/2024 11:59 PM
Forum Assessment Format: Individual Short Extension: Yes (3 days)	20%	
Mini Project Assessment Format: Individual Short Extension: Yes (3 days)	50%	Due Date: 28/10/2024 11:59 PM

Assessment Details

Online Quizzes

Course Learning Outcomes

- CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program
- CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment

Detailed Assessment Description

This will be done online and will cover the course material and specific readings.

Privacy Impact Assessment

Course Learning Outcomes

- CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program

- CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment

Detailed Assessment Description

During the course you will examine the scope and complexity of assessing and communicating Risk and related compliance issues. This first assignment is designed to focus your thinking on one particular area of this broad domain of knowledge.

Forum

Course Learning Outcomes

- CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program
- CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment
- CLO3 : Apply theory to implement risk mitigation security controls throughout an organisation and perform a business impact analysis

Detailed Assessment Description

Students will be required to participate in an online discussion by first responding to, commenting on, or providing an opinion about an online article or technical report in terms of given criteria. They will then need review the responses made by other students and post a further (second) comment responding to the initial posting by another student; again, with reference to the given criteria (refuting, agreeing, explaining, expanding etc).

Mini Project

Course Learning Outcomes

- CLO1 : Explain basic concepts, i.e. compliance laws, standards, best practices and policies, of risk management, the need for risk management for businesses and organisations, approaches of mitigating risk by managing threats, vulnerabilities and exploits, and essential components of an effective organisational risk management program
- CLO2 : Investigate techniques for detecting, identifying and analysing assets' and processes' potential threats, vulnerabilities, and exploits within an organisation, and the process of performing a risk assessment
- CLO3 : Apply theory to implement risk mitigation security controls throughout an organisation and perform a business impact analysis
- CLO4 : Undertake a computer incident response team (CIRT), a business continuity plan (BCP) and a disaster recovery plan (DRP) based on the evaluation of a risk

assessment for an organisation

Detailed Assessment Description

Students will develop a comprehensive formal risk management strategy for a hypothetical organisation. In so doing, they will incorporate and apply the concepts learned in the course and will also be required to undertake further independent research to identify, assess, understand and articulate in both technical and business terms, the risks, solutions and security controls that should form part of the proposed strategy.

Details of the mini project will be given in week 5 and students will then be able to start working on this. In so doing, students will gain an overall understanding of risk management, its importance, and critical processes required when building such a formal risk management plan. In addition, they will have the opportunity to conduct independent research, evaluation and analysis of risk mitigation and risk prevention technologies, techniques and controls.

General Assessment Information

Use of Generative AI in Assessments

As this assessment task involves some planning or creative processes, you are permitted to use software to generate initial ideas. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., only occasional AI-generated words or phrases may form part of your final submission. It is a good idea to keep copies of the initial prompts to show your lecturer if there is any uncertainty about the originality of your work.

If the outputs of generative AI, such as ChatGPT form a part of your submission, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension, and exclusion.

** To cite: OpenAI (Year Accessed). ChatGPT. OpenAI. https://openai.com/models/chatgpt/*

* Please note that the outputs from these tools are not always accurate, appropriate, or properly referenced. Before submission, you should ensure that you have moderated and critically evaluated the outputs from generative AI tools such as ChatGPT

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Introduction and overview - risk management concepts, principles and practices
Week 2 : 22 July - 26 July	Lecture	Understanding risk, threats and vulnerabilities - the nature of cyber-attacks, malware and malicious behaviour
Week 3 : 29 July - 2 August	Lecture	The anatomy of a cyber-attack -What happens you're your organisation is targeted?
Week 4 : 5 August - 9 August	Lecture	Assessing and analysing risk -Identifying assets, threats and vulnerabilities. Threat modelling and evaluation approaches.
	Assessment	
Week 5 : 12 August - 16 August	Lecture	Developing a risk management strategy - Organisational needs, requirements, objectives, constraints, policies.
Week 6 : 19 August - 23 August	Assessment	
	Lecture	Threat prevention and mitigation - Security controls - technical, human, physical
Week 7 : 9 September - 13 September	Lecture	Developing security policy, end user training.
	Assessment	
Week 8 : 16 September - 20 September	Assessment	
	Lecture	Performing a risk assessment -scope, methodologies, evaluation, cost benefit analysis
Week 9 : 23 September - 27 September	Assessment	
	Lecture	Standards, guidelines and compliance.
Week 10 : 30 September - 4 October	Lecture	Cloud computing - Risk or Remedy - where does this fit in?
Week 11 : 7 October - 11 October	Lecture	Business Impact Analysis and developing an overall strategy
Week 12 : 14 October - 18 October	Assessment	
	Lecture	Business Continuity and Disaster Recovery planning
Week 13 : 21 October - 25 October	Lecture	Review and summary
	Assessment	

Attendance Requirements

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

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	HUADONG MO		R118, Building 20	0251145183	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
	Michael Mc Garity					No	No

Other Useful Information

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 4pm, Mon to Fri)