UNSW Course Outline

ZEIT8032 Information Assurance Principles - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8032
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

This ZEIT8032 Information Assurance Principles course is one of the core courses for Masters in Cybersecurity Operations (8629). It is also offered as an elective for other programs at UNSW Canberra. Additionally, we extend our offer to students in the Homeland Security Program at

Arizona State University (ASU), who will enrol in this course as part of the PLuS Alliance (PLuS Alliance is a strategic alliance between ASU, UNSW and King's College London, designed to help increase educational opportunities for students at each of the partner institutions by offering global experiences and opportunities for interacting and collaborating with global virtual teams. The PLuS online course exchange is an initiative among PLuS Alliance institutions that allows students from the three institutions to take online courses or modules offered at any one of the PLuS Alliance institutions.) online course exchange.

The aim of this course is to provide insights into modern cyber security threats and defensive controls and explore effective computer security and risk management strategies, with particular emphasis on Information Assurance (IA) practices and techniques.

The course provides a graduate-level foundation in IA for a diverse audience, from middle-level managers to executives. It caters to those with both non-technical and technical backgrounds, and those from a variety of government, commercial and non-for-profit organisations.

This course explores concepts such as layered defence mechanisms, use of several technologies in multiple instances (true defence in depth), threat/risk identification, and mitigation and incident response techniques.

It will enable executive-level managers to more fully understand the real-world challenges faced by their cyber security teams today. It will assist in developing the frameworks and policies, and in supporting the evidence-based decisions, that are required to allow teams to protect their environments efficiently. It will also increase understanding of the resulting costs and benefits.

It is a standard postgraduate course, available only through distance delivery mode, worth six units of credit (6 UOC) and requires 160 hrs of student study time. There are no prerequisites, but it is expected that enrolling students can: understand emerging technologies; explain specific technical terms; describe problems in technical and non- technical language.

Course Aims

This introductory course aims to provide insight on cyber security threats, practices and controls. This course will explore concepts such as layered defence mechanisms using different technologies and multiples thereof (true defence in depth), threat/risk identification and mitigation and incident response techniques.

This course will enable executive level management to properly understand the real world

challenges faced by their Cyber Security teams today. Also to assist in the development of the frameworks, policies and the evidence based decisions required to allow their teams to protect their environments efficiently and to understand the resulting costs and benefits.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions that are essential for implementing an effective IA program.
CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.
CLO3 : Explain mechanisms for detecting cyber incidents and anomalies as they occur; suggest the various controls that organisations could consider and suggest recovery processes.
CLO4 : Apply IA principles, methodologies and frameworks and provide the relevant advice required by security personnel for effective cyber security plans.

Course Learning Outcomes	Assessment Item
CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions that are essential for implementing an effective IA program.	• Forum Discussion (Initial) • Forum Discussion (Replies) • Group report • Executive Summary
CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.	• Forum Discussion (Initial) • Forum Discussion (Replies) • Group report • Executive Summary
CLO3 : Explain mechanisms for detecting cyber incidents and anomalies as they occur; suggest the various controls that organisations could consider and suggest recovery processes.	• Group report • Executive Summary
CLO4 : Apply IA principles, methodologies and frameworks and provide the relevant advice required by security personnel for effective cyber security plans.	• Executive Summary

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate | Microsoft Teams

Learning and Teaching in this course

This course is delivered in distance mode and uses Moodle for students' online engagements. Instructions will be provided for each module in the course Moodle site, explaining what is expected within each topic. We expect all students to use Moodle, which provides mechanisms to facilitate online discussions between students and with the lecturer.

You must log on to Moodle frequently for updates about the course. It is expected that you will study as much of the recommended reading material as you can, and expand your reading through the linked references and your own research. Reflect on the material and think outside the box to help comprehension of the concepts and techniques taught in this course.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Forum Discussion (Initial) Assessment Format: Individual Short Extension: Yes (7 days)	15%	Due Date: 04/08/2024 11:59 PM
Forum Discussion (Replies) Assessment Format: Individual Short Extension: Yes (7 days)	25%	Due Date: 18/08/2024 11:59 PM
Group report Assessment Format: Group	25%	Due Date: 06/10/2024 11:59 PM
Executive Summary Assessment Format: Individual Short Extension: Yes (7 days)	35%	Due Date: 03/11/2024 11:59 PM

Assessment Details

Forum Discussion (Initial)

Assessment Overview

This assessment is related to Autonomous Operations. It will assess students' knowledge gained during first study weeks. Students are required to address a specific question, and conduct further analyses and deeper research into a specific task. Required online reading materials, and research papers will be provided in Moodle. This material plus students' own additional research on the Internet will provide essential background for the assignment. Students participate in the discussion forums – in Forum they reflect and build on instructors' and fellow students' comment.

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions that are essential for implementing an effective IA program.
- CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.

Detailed Assessment Description

Autonomous Operations will assess students' knowledge gained during first study weeks. Students are required to address a specific question, and conduct further analyses and deeper research into a specific task. Required online reading materials, and research papers will be provided in Moodle. This material plus students' own additional research on the Internet will provide essential background for the assignment. Students participate in the discussion forums – in Forum 1 they reflect and build on instructors' and fellow students' comments.

Assignment submission Turnitin type

This is not a Turnitin assignment

Forum Discussion (Replies)

Assessment Overview

Fellow students are required to assess the posts submitted by their classmates and leave the comments based on the reading materials and research papers that you read.

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions that are essential for implementing an effective IA program.
- CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.

Detailed Assessment Description

Autonomous Operations will assess students' knowledge gained during first study weeks. Students are required to address a specific question, and conduct further analyses and deeper research into a specific task. Required online reading materials, and research papers will be provided in Moodle. This material plus students' own additional research on the Internet will provide essential background for the assignment. Students participate in the discussion forums – in Forum 1 they reflect and build on instructors' and fellow students' comments.

Assignment submission Turnitin type

This is not a Turnitin assignment

Group report

Assessment Overview

The Case Study has two parts. Students will develop knowledge by evaluating a particular case study. This assessment is the first part. Students discuss the case study within the group. This includes joining the tutorial discussion and then reflect on the skills they have gained to demonstrate them in a group report. Online readings from books and papers will be provided in Moodle. This material, plus students' additional research, will provide essential preparation and background for this assessment.

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions that are essential for implementing an effective IA program.
- CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.
- CLO3 : Explain mechanisms for detecting cyber incidents and anomalies as they occur; suggest the various controls that organisations could consider and suggest recovery processes.

Detailed Assessment Description

Case Study has two parts. Students will develop knowledge by evaluating a particular case study. First, students discuss the case study within the group. This includes joining the tutorial discussion and then reflects on the skills. They have gained to demonstrate them in a group report. Second, an individual component – the executive summary – builds on instructors' comments, and will require further, deeper research into the case study. Online readings from books and papers will be provided in Moodle. This material, plus students' additional research, will provide essential preparation and background for this assignment.

Assignment submission Turnitin type

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

Executive Summary

Assessment Overview

The Case Study has two parts. Students will develop knowledge by evaluating a particular case study. This assessment is the second part, an individual component – the executive summary – builds on instructors' comments, and will require further, deeper research into the case study.

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components, and definitions

that are essential for implementing an effective IA program.
- CLO2 : Investigate preventive controls that organisations should consider when developing strategies to minimise cyber security risks.
- CLO3 : Explain mechanisms for detecting cyber incidents and anomalies as they occur; suggest the various controls that organisations could consider and suggest recovery processes.
- CLO4 : Apply IA principles, methodologies and frameworks and provide the relevant advice required by security personnel for effective cyber security plans.

Detailed Assessment Description

Case Study has two parts. Students will develop knowledge by evaluating a particular case study. First, students discuss the case study within the group. This includes joining the tutorial discussion and then reflects on the skills. they have gained to demonstrate them in a group report. Second, an individual component – the executive summary – builds on instructors' comments, and will require further, deeper research into the case study. Online readings from books and papers will be provided in Moodle. This material, plus students' additional research, will provide essential preparation and background for this assignment.

Assignment submission Turnitin type

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

General Assessment Information

All marks obtained for assessment items during the session are provisional. The feedback on each assessment will be provided within 10 working days after the due date. The final mark as published by the University following the assessment review group meeting is the only official mark. Major end-of-semester assignments will not be released to the students until the course final results are reviewed by the School and approved.

No extensions are possible without a formal request for special consideration (see policy link on Moodle). The penalty for late submission will be 10% per calendar day, or part thereof unless prior special consideration has been granted. Assessment items submitted more than 5 calendar days late will not be assessed and will receive a grade of zero.

All requests for special consideration must be formally submitted via MyUNSW before the assessment due date.

Grading Basis

Standard

Requirements to pass course

The four assessment items form the requirements to complete this subject. To pass this subject, students must participate in all assignment components for Autonomous Operations and Case Study and must achieve at least 50 marks out of a total of 100 marks for these two components.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Introduction: The need for IA
Week 2 : 22 July - 26 July	Lecture	IA strategy, principles and concepts
Week 3 : 29 July - 2 August	Lecture	IA management, current practices, and regulations
	Assessment	Assessment 1: Initial Post due 04/08/2024 at 11:59pm
Week 4 : 5 August - 9 August	Lecture	Approaches to implement IA and organisational structures; IA asset management
Week 5 : 12 August - 16 August	Lecture	IA risk management, policy, and processes
	Assessment	Assessment 2: Post replies due 18/08/2024 at 11:59pm
Week 6 : 19 August - 23 August	Lecture	IA evaluation, certification and accreditation
	Tutorial	Tutorial 1
Week 7 : 9 September - 13 September	Lecture	Role of IA in a system development life cycle
	Tutorial	Tutorial 2
Week 8 : 16 September - 20 September	Lecture	Different types of IA Controls Internet access control; physical and environmental controls.
	Tutorial	Tutorial 3
Week 9 : 23 September - 27 September	Lecture	IA preventive tools and techniques
	Tutorial	Tutorial 4
Week 10 : 30 September - 4 October	Lecture	IA monitoring, computer forensics, incident handling
	Assessment	Assessment 3: Case Study (Group Report) Due 06/10/2025 at 11:59pm
Week 11 : 7 October - 11 October	Lecture	Business continuity; backup and restoration IA measurements and metrics
Week 12 : 14 October - 18 October	Lecture	Course overview and recap

Attendance Requirements

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

Course Resources

Prescribed Resources

You will need ongoing access to the following book to complete this course. The library does not hold multiple copies of the nominated text. It is recommended that you purchase the book as either a hard copy or a Kindle version.

Information Assurance: Effective Computer Security and Risk Management Strategies
Corey Schou and Steven Hernandez, McGraw Hill, 2015, ISBN-13: 978-007182165-0

Recommended Resources

A variety of additional resource materials will be made available. These consist of:

- Recommended papers and selected chapters from textbooks, Internet-based documents and other sources. In general, these materials will be available through the Moodle pages.
- Videos, 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.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Siqi Ma					No	Yes

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)