UNSW Course Outline

INFS1701 Introduction to Networking and Security - 2024

Published on the 25 Aug 2024

General Course Information

Course Code : INFS1701
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : UNSW Business School
Academic Unit : School of Information Systems and Technology Management
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

IT infrastructure and security are essential for the smooth operation of businesses in today's digital world. As businesses increasingly rely on technology, the need for skilled IT professionals who can design, implement, and manage secure IT systems is growing. In this course, you will

gain a deep understanding of information technology infrastructure and security in the business environment. You will develop skills and foundational knowledge to pursue a career in cybersecurity or other related fields. You will learn the different components of IT infrastructure and security, as well as the best practices for designing, implementing, and managing secure systems. As you learn more about IT infrastructure and security, you will gain a deeper appreciation for the importance of the 'People, Processes, and Technology' components of cybersecurity. By completing this course, you will develop the prerequisite skills and knowledge required to enrol in the Level 2 intermediate IS course – INFS2701.

Course Aims

This course aims to help you develop a fundamental understanding about networking infrastructure and cybersecurity You will get an opportunity to engage with a diverse range of cybersecurity topics as it relates to modern, highly connected workplaces. You will gain important knowledge and skills to undertake more advanced courses in cybersecurity management, governance and could architecture.

Course Learning Outcomes

Course Learning Outcomes	Program learning outcomes
CLO1 : Apply knowledge of the current architecture of the Internet and the entities involved with the day-to-day running of networking technologies to solve real-world problems.	• PLO1 : Business Knowledge
CLO2 : Explain and apply principles of networking and cybersecurity in various business contexts.	• PLO1 : Business Knowledge • PLO3 : Business Communication
CLO3 : Create practical solutions based on your knowledge of business data networks, frameworks and regulations and their security that demonstrate analytical and practical skills.	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication
CLO4 : Analyse relevant technical and managerial considerations related to the design, deployment, ethics and/or the uses of secure networking technologies within various business contexts.	• PLO1 : Business Knowledge • PLO4 : Teamwork • PLO5 : Responsible Business Practice
CLO5 : Collaborate effectively with teammates in a culturally diverse environment to achieve project goals.	• PLO1 : Business Knowledge • PLO4 : Teamwork • PLO5 : Responsible Business Practice

Course Learning Outcomes	Assessment Item
CLO1 : Apply knowledge of the current architecture of the Internet and the entities involved with the day-to-day running of networking technologies to solve real-world problems.	• Final Exam • Group Project • Tutorial Work
CLO2 : Explain and apply principles of networking and cybersecurity in various business contexts.	• Final Exam • Group Project • Tutorial Work
CLO3 : Create practical solutions based on your knowledge of business data networks, frameworks and regulations and their security that demonstrate analytical and practical skills.	• Final Exam • Group Project • Tutorial Work
CLO4 : Analyse relevant technical and managerial considerations related to the design, deployment, ethics and/or the uses of secure networking technologies within various business contexts.	• Final Exam • Group Project
CLO5 : Collaborate effectively with teammates in a culturally diverse environment to achieve project goals.	• Tutorial Work • Group Project

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360

Learning and Teaching in this course

The classes in this course will be interactive. You are expected to do all pre-class activities and come prepared to engage with your peers and the teaching staff.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Program learning outcomes
Final Exam Assessment Format: Individual	50%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO2 : Problem Solving • PLO3 : Business Communication
Group Project Assessment Format: Group	30%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO4 : Teamwork • PLO5 : Responsible Business Practice
Tutorial Work Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: Not Applicable	• PLO1 : Business Knowledge • PLO3 : Business Communication • PLO5 : Responsible Business Practice

Assessment Details

Final Exam

Assessment Overview

A formal examination will take place during the University Exam Period. The examination is worth 50% of the total marks for this course. You must plan to be available for the full examination period to attend the final exam. In addition, you should also ensure that you will be available for a supplementary examination in the event of illness or misadventure. All material covered in lectures, tutorials, exercises, and set readings is examinable. All exams are conducted in accordance with the UNSW Rules for the Conduct of Examinations and it is your responsibility to be familiar with these rules.

Assesses: PLO1, PLO2, PLO3, PLO5, PLO6

Course Learning Outcomes

- CLO1 : Apply knowledge of the current architecture of the Internet and the entities involved with the day-to-day running of networking technologies to solve real-world problems.
- CLO2 : Explain and apply principles of networking and cybersecurity in various business contexts.
- CLO3 : Create practical solutions based on your knowledge of business data networks, frameworks and regulations and their security that demonstrate analytical and practical skills.

- CLO4 : Analyse relevant technical and managerial considerations related to the design, deployment, ethics and/or the uses of secure networking technologies within various business contexts.

Assessment Length

3 hours

Assessment information

More information will be provided during classes.

Assignment submission Turnitin type

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

Generative AI Permission Level

Planning/Design Assistance

You are permitted to use generative AI tools, software or services to generate initial ideas, structures, or outlines. 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 tool, software or service should not be a part of your final submission. You should keep copies of your iterations to show your Course Authority if there is any uncertainty about the originality of your work.
If your Convenor has concerns that your answer contains passages of AI-generated text or media 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 and media 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 UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Group Project

Assessment Overview

This assessment requires you to develop a strategy and transformation roadmap based on in-depth research.

Assesses: PLO1, PLO2, PLO3, PLO4, PLO5, PLO6
BCom point: PLO6

Course Learning Outcomes

- CLO1 : Apply knowledge of the current architecture of the Internet and the entities involved

with the day-to-day running of networking technologies to solve real-world problems.
- CLO2 : Explain and apply principles of networking and cybersecurity in various business contexts.
- CLO3 : Create practical solutions based on your knowledge of business data networks, frameworks and regulations and their security that demonstrate analytical and practical skills.
- CLO4 : Analyse relevant technical and managerial considerations related to the design, deployment, ethics and/or the uses of secure networking technologies within various business contexts.
- CLO5 : Collaborate effectively with teammates in a culturally diverse environment to achieve project goals.

Detailed Assessment Description

This assessment requires you to work in small groups to solve a real-world challenge. More information about this assessment will be provided in class.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.
If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Tutorial Work

Assessment Overview

You will engage in interactive problem-solving and discussions and complete hands-on tasks that will develop your cybersecurity skills. Students are required to prepare and participate in tutorials.

Assesses: PLO1, PLO2, PLO4, PLO5, PLO6

BCom point: PLO5

Course Learning Outcomes

- CLO1 : Apply knowledge of the current architecture of the Internet and the entities involved with the day-to-day running of networking technologies to solve real-world problems.
- CLO2 : Explain and apply principles of networking and cybersecurity in various business contexts.
- CLO3 : Create practical solutions based on your knowledge of business data networks, frameworks and regulations and their security that demonstrate analytical and practical skills.
- CLO5 : Collaborate effectively with teammates in a culturally diverse environment to achieve project goals.

Detailed Assessment Description

For this assessment you are required to attend all tutorial classes and complete the in-class activities to get feedback from your tutor.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Assistance with Attribution

This assessment requires you to write/create a first iteration of your submission yourself. You are then permitted to use generative AI tools, software or services to improve your submission in the ways set out below.
Any output of generative AI tools, software or services that is used within your assessment must be attributed with full referencing.
If outputs of generative AI tools, software or services form part of your submission and are not appropriately attributed, your Convenor will determine whether the omission is significant. If so, you may be asked to explain your submission. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

General Assessment Information

More information about the assessments will be provided in class.

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 0 : 2 September - 8 September	Activity	Read Course Outline
Week 1 : 9 September - 15 September	Lecture	Introductions: • Course • Teaching staff • Assessments Fundamentals of Networking (Part1) Tutorial
Week 2 : 16 September - 22 September	Lecture	Fundamentals of Networking (Part II) Tutorial
Week 3 : 23 September - 29 September	Lecture	Fundamentals of Cybersecurity (I) Tutorials
Week 4 : 30 September - 6 October	Lecture	Fundamentals of Cyber Security (Part II) Tutorial
Week 5 : 7 October - 13 October	Activity	Since Monday of this week is a public holiday, the lecture will be recorded and an interactive activity will be provided. More information will be given in the weeks leading up to this week. The People, Processes, and Technology of cyber security (Part I - the People component) Tutorial
Week 6 : 14 October - 20 October	Activity	Flexibility Week Please review topics from week 1 to week 5 Work on your group project
Week 7 : 21 October - 27 October	Lecture	The People, Processes, and Technology of cyber security (Part II - the Processes component) Tutorial
Week 8 : 28 October - 3 November	Lecture	The People, Processes, and Technology of cyber security (Part III - the Technology component) Tutorial
Week 9 : 4 November - 10 November	Lecture	Responsible Management of Technologies (Part I) Tutorial
Week 10 : 11 November - 17 November	Lecture	Responsible Management of Technologies (Part II) Group Project due Group Presentation Tutorial
Week 11 : 18 November - 24 November	Lecture	Introductions: • Course • Teaching staff • Assessments Fundamentals of Networking (Part1) Tutorial

Attendance Requirements

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

Course Resources

Prescribed Resources

All resources will be provided via Moodle, however you are encouraged to do your own further research on the topics to develop higher understanding of the topics.

Course Evaluation and Development

We will seek you feedback in ways we can improve this course for your and future offerings. This will be done through a mid-term feedback and an end of term myExperience survey.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Pranit Anand		2076	93481398	Tuesdays 10 to 11, Fridays 9 to 10	No	Yes

Other Useful Information

Academic Information

COURSE POLICIES AND SUPPORT

The Business School expects that you are familiar with the contents of this course outline and the UNSW and Business School learning expectations, rules, policies and support services as listed below:

- Program Learning Outcomes
- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Protocol for Viewing Final Exam Scripts
- Student Learning Support Services

Further information is provided on the Policies and Guidelines page.

Students may not circulate or post online any course materials such as handouts, exams, syllabi or similar resources from their courses without the written permission of their instructor.

STUDENT LEARNING OUTCOMES

The Course Learning Outcomes (CLOs) – under the Outcomes tab – are what you should be able to demonstrate by the end of this course, if you participate fully in learning activities and successfully complete the assessment items.

CLOs also contribute to your achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to UNSW graduate capabilities. More information on Coursework PLOs is available on the Policies and Guidelines page. For PG Research PLOs, including MPDBS, please refer to UNSW HDR learning outcomes.

Academic Honesty and Plagarism

As a student at UNSW you are expected to display academic integrity in your work and interactions. Where a student breaches the UNSW Code of Conduct with respect to academic integrity, the University may take disciplinary action. To assure academic integrity, you may be required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Code of Conduct, it is strongly recommended that you complete the Working with Academic Integrity module before submitting your first assessment task. It is a free, online self-paced Moodle module that should take about one hour to complete.

Submission of Assessment Tasks

SHORT EXTENSIONS

Short Extension is a new process that allows you to apply for an extended deadline on your assessment without the need to provide supporting documentation, offering immediate approval during brief, life-disrupting events. Requests are automatically approved once submitted.

Short extensions are ONLY available for some assessments. Check your course outline or Moodle to see if this is offered for your assessments. Where a short extension exists, all students enrolled in that course in that term are eligible to apply. Further details are available the UNSW Current Students page.

SPECIAL CONSIDERATION

You can apply for special consideration when illness or other circumstances beyond your control interfere with your performance in a specific assessment task or tasks, including online exams. Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable.

Applications can only be made online and will NOT be accepted by teaching staff. Applications will be assessed centrally by the Case Review Team, who will update the online application with the outcome and add any relevant comments. The change to the status of the application immediately sends an email to the student and to the assessor with the outcome of the application. The majority of applications will be processed within 3-5 working days.

For further information, and to apply, see Special Consideration on the UNSW Current Students page.

LATE SUBMISSION PENALTIES

LATE SUBMISSION PENALTIES

For assessments other than examinations, late submission will incur a penalty of 5% per day or part thereof (including weekends) from the due date and time. An assessment will not be accepted after 5 days (120 hours) of the original deadline unless special consideration has been approved. In the case of an approved Equitable Learning Plan (ELP) provision, special consideration or short extension, the late penalty applies from the date of approved time extension. After five days from the extended deadline, the assessment cannot be submited.

An assessment is considered late if the requested format, such as hard copy or electronic copy, has not been submitted on time or where the 'wrong' assessment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, the LIC may stipulate a different penalty. Details of such late penalties will be available on the course Moodle page.

FEEDBACK ON YOUR ASSESSMENT TASK PERFORMANCE

Feedback on student performance from formative and summative assessment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than a final assessment, will be assessed and students provided with feedback, with or without a provisional result, within 10 working days of submission, under normal circumstances. Feedback on continuous assessment tasks (e.g. laboratory and studio-based, workplace-based, weekly quizzes) will be provided prior to the midpoint of the course.

Faculty-specific Information

PROTOCOL FOR VIEWING FINAL EXAM SCRIPTS

UNSW students have the right to view their final exam scripts, subject to a small number of very specific exemptions. The UNSW Business School has set a protocol under which students may view their final exam script. Individual schools within the Faculty may also set up additional local processes for viewing final exam scripts, so it is important that you check with your School.

If you are completing courses from the following schools, please note the additional school-specific information:

- Students in the **School of Accounting, Auditing & Taxation** who wish to view their final examination script should also refer to this page.
- Students in the **School of Banking & Finance** should also refer to this page.
- Students in the **School of Information Systems & Technology Management** should also refer to this page.

COURSE EVALUATION AND DEVELOPMENT

Feedback is regularly sought from students and continual improvements are made based on this feedback. At the end of this course, you will be asked to complete the myExperience survey, which provides a key source of student evaluative feedback. Your input into this quality enhancement process is extremely valuable in assisting us to meet the needs of our students and provide an effective and enriching learning experience. The results of all surveys are carefully considered and do lead to action towards enhancing educational quality.

QUALITY ASSURANCE

The Business School is actively monitoring student learning and quality of the student experience in all its programs. A random selection of completed assessment tasks may be used for quality assurance, such as to determine 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 Business School programs. All material used for such processes will be treated as confidential.

TEACHING TIMES AND LOCATIONS

Please note that teaching times and locations are subject to change. Students are strongly advised to refer to the Class Timetable website for the most up-to-date teaching times and locations.