# CSIT988
# Security, Ethics and Professionalism

## Week 1: Introduction and Overview of the Subject

**Subject Coordinator:** *Dr Khoa Nguyen*

**School of Computing and Information Technology**

**Autumn 2025**

# Acknowledgement of Country

“We acknowledge that Country for Aboriginal peoples is an interconnected set of ancient and sophisticated relationships. The University of Wollongong spreads across many interrelated Aboriginal Countries that are bound by the sacred landscape, an intimate relationship with that landscape since creation. From Sydney, to the Southern Highlands, to the South Coast; from freshwater, to bitter water, to salt; from city, to urban, to rural, the University of Wollongong acknowledges the custodianship of the Aboriginal peoples of this place and space that has kept alive the relationships between all living things. The University acknowledges the devastating impact of colonisation on our campuses footprint and commit ourselves to truth telling, healing and education.”

# Stay in the know...

## Keep connected at UOW

Discover the student systems and communication channels you'll use both on campus and at home.

UOWMail

SOLS

AskUOW

MyUOW

Moodle

Instagram

Website

# Health and Safety Information for Students

Commencement of Session

UNIVERSITY OF WOLLONGONG AUSTRALIA

# What to do in an emergency?

**KEEP CALM – STAY SAFE**

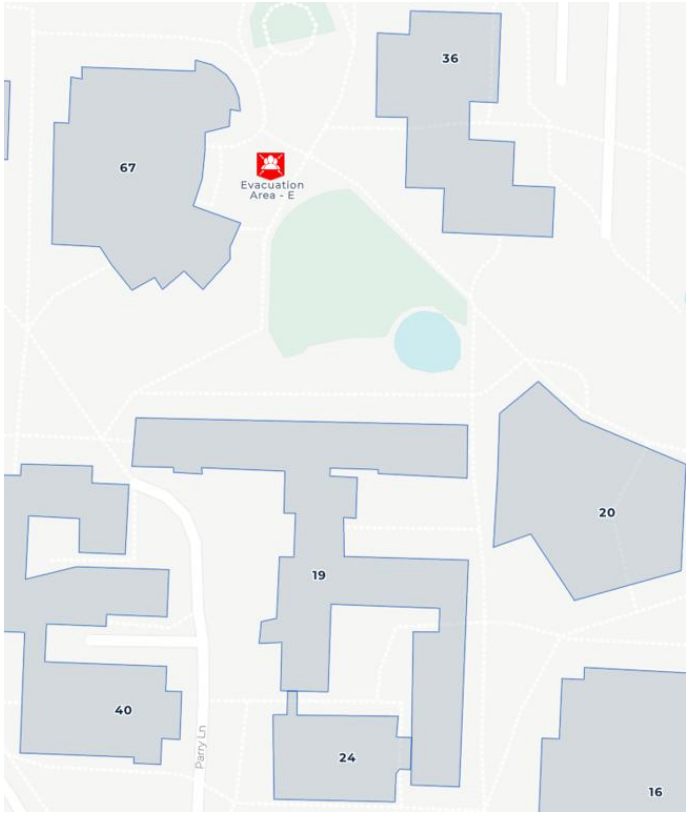
If the alarm sounds or you are notified to evacuate:

- Follow instructions of building warden or staff member
- Leave by the nearest safe emergency exit
- Proceed to your emergency evacuation assembly point
- Await further instructions
- Do not return to the building until it is safe to do so

If required to take shelter:

- Follow instructions of building warden or staff member
- Lock doors, close windows/blinds and seek refuge
- Await further instructions

**The nearest assembly area for this building is:**

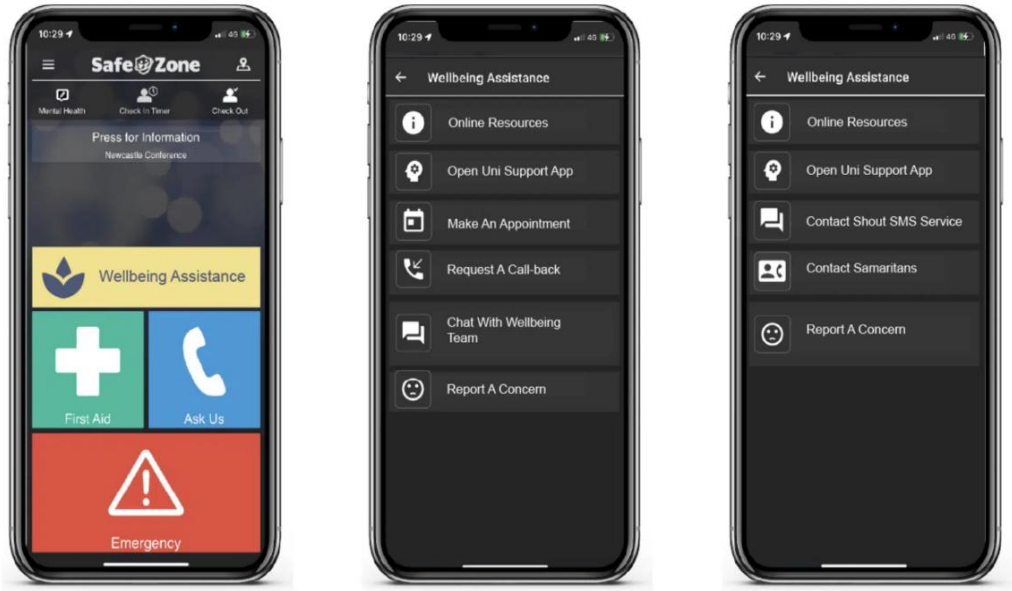


# Need assistance on campus?

**WE ARE HERE TO HELP**

If you require first aid or medical assistance while on campus:

- Locate a first aid officer, or
- Call UOW Security on 4221 4900, or
- Use Wellbeing Assistance, First Aid or Emergency buttons on SafeZone App available free for iOS, Android and Windows.



# Reporting hazards

## KEEPING YOUR UNIVERSITY SAFE AND COMFORTABLE

If you notice any hazards (e.g. broken furniture or equipment) in your teaching area or anywhere on Campus:

- Report it to your Lecturer/Tutor/Supervisor
- The University has an online hazard and incident reporting tool called SafetyNet
- Report IT equipment hazards to Information Management and Technology Services on 4221 3000
- Report building and grounds hazards to Infrastructure and Property Division 4221 3217

# Smoke-Free University

## SAY GOODBYE TO SECONDHAND SMOKE

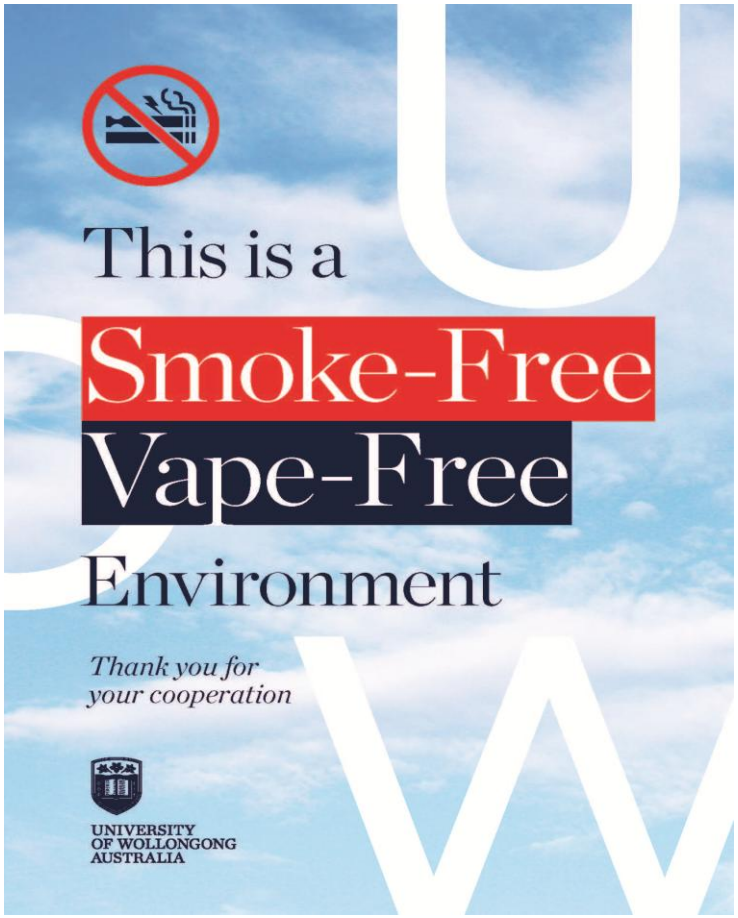
All UOW public areas including buildings, eating areas, grounds, pathways and transport stops have been smoke-free since July 2016.

This includes the use of vapes and e-cigarettes.

Please co-operate with this policy to help make our campus healthier for everyone.

For more information:

uow.info/smoke-free



U O W

For more information: uow.info/safe-at-work

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# Overview of the Subject

# Contact Details

**Dr Khoa NGUYEN**

- Office: 3.213
- Email: khoa@uow.edu.au
- Subject title starts with [CSIT988]
- Consultation hours:
  - Monday 10:30 -- 12:30
  - Thursday 12:30 -- 14:30

  Either face-to-face (at my office) or online (via Zoom).

  It is preferred that you send me an email to book an appointment in advance.

# About Me

- 2014: PhD in Cryptography at Nanyang Technological University (NTU), Singapore
- 2014-2021: (Senior) Researcher at NTU
- August 2021– present: Senior Lecturer, SCIT, UOW
- Subject coordinator of CSIT988 since 2022

- Research Areas: Cryptography, Information Security and Cybersecurity, in particular:
  - Privacy-preserving cryptographic protocols
  - Applications of cryptography to Blockchain and Big Data
  - Interplay between Cryptography and Machine Learning

- More information: https://sites.google.com/view/khoantt/

# eLearning - Moodle

- The UOW eLearning system (Moodle) will be used extensively throughout the course.
  - Announcements
  - Lecture slides and records, workshop exercises
  - Assessment details
  - Discussion forums
  - Polls, quizzes
- Students should regularly check the subject's Moodle site

https://moodle.uowplatform.edu.au/course/view.php?id=42919,

as important information, including details of unavoidable changes in assessment requirements will be posted from time to time via e-Learning space. Any information posted to Moodle is deemed to have been notified to all students.

# Subject Description

This subject aims to provide students with a deep understanding of the security, risk management, and professional practice aspects, including ethical and social issues, of enterprises and organisations in the digital world. In today's world, organisations must be prepared to defend against threats in digital space. Decision-makers must be familiar with the principles and best practices of information security to better protect their organisations. This subject covers key issues in information security management, including security options, ethical and social issues, best practices, the regulatory environment and Government policy, risk management and control.

# Subject Learning Outcomes

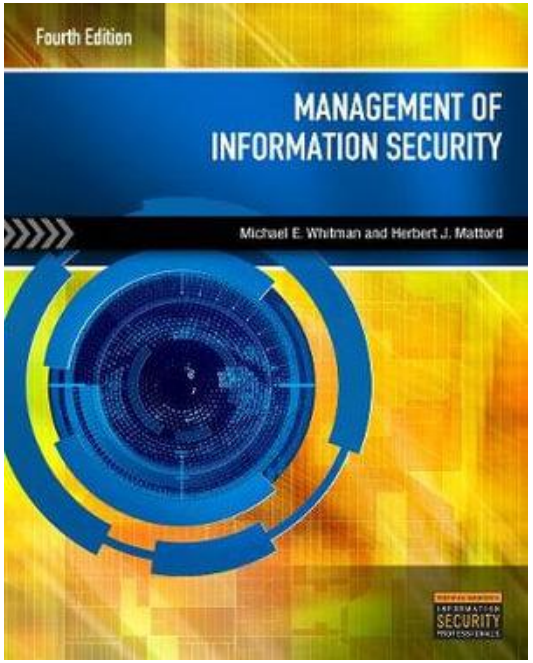
1. Apply the security system development life cycle to create a comprehensive security posture.
2. Implement effective information security planning, including contingency planning.
3. Analyse emerging trends in information security management practices.
4. Implement information security planning against current security issues in digital applications.
5. Evaluate and interpret ethical and professional issues at different levels.
6. Critically analyse and adopt risk management techniques to identify, prioritise, and control risks.

# Textbook

**Management of Information Security**

Authors: **Michael Whitman** and **Herbert Mattord**

Available at UOW Library: hard copy (**4th edition**), e-book (6th edition)



# Other Resources

- Michael E. Whitman, Herber J. Mattord, **Readings and Cases in Information Security: Law and Ethics**, Cengage Learning, 2010.

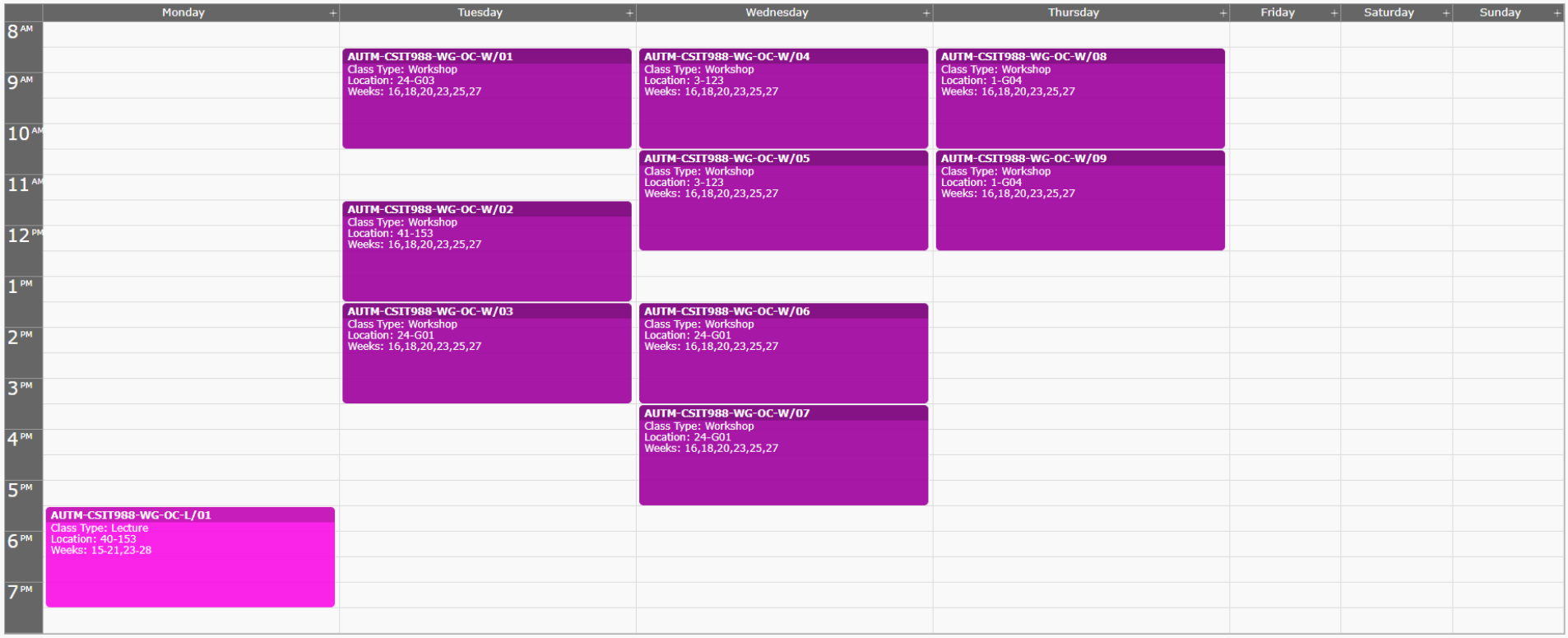
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, **Security in Computing**, 5th Edition, Pearson, 2015.

- William Stallings, Lawrie Brown**, Computer Security: Principles and Practice**, 4th Edition, Pearson, 2017.

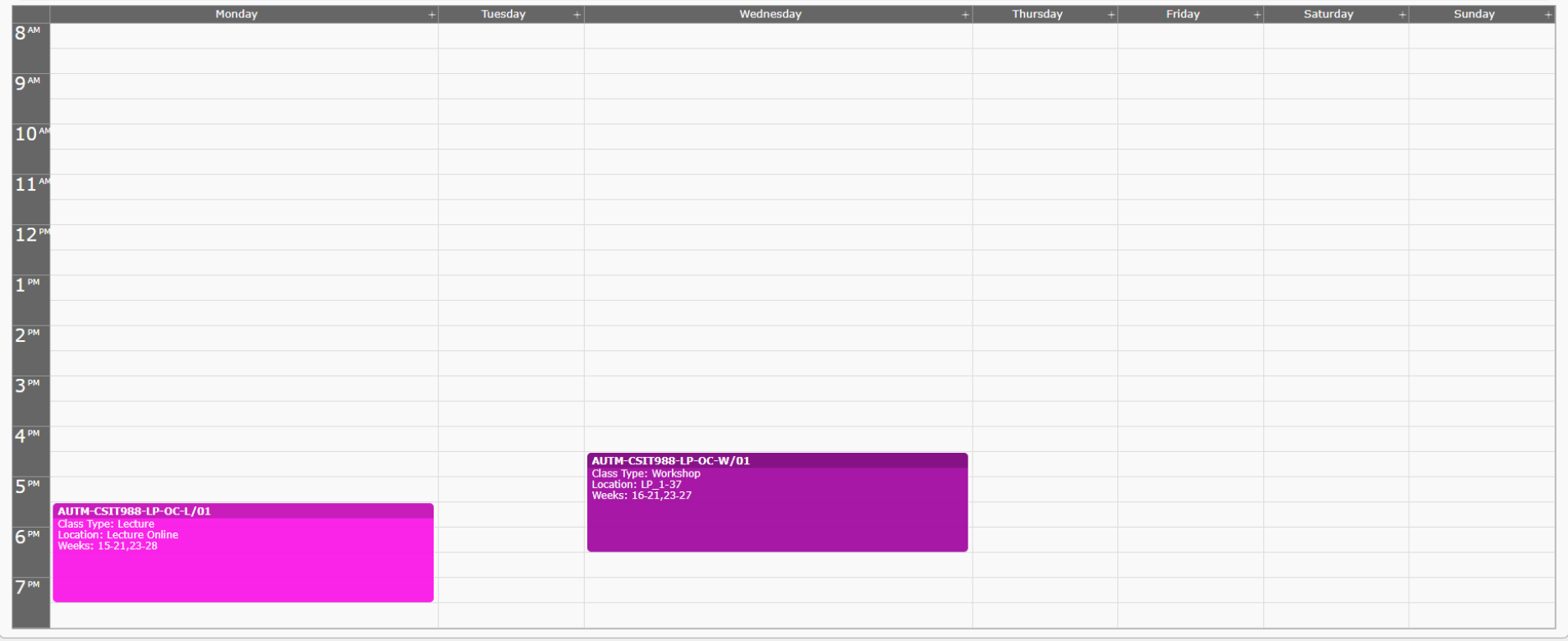
- **The Cyber Security Body of Knowledge**, Version 1.1.0, The National Cyber Security Centre, 2021. Available at https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

| Week | Lecture Topic(s) | Reading(s) | Workshop |
|---|---|---|---|
| **1** | Introduction and Overview of the Subject | SO + Chapter 1 | |
| 2 | Information Security Management | Chapter 1 | W01 |
| 3 | Planning for Security | Chapter 2 | |
| 4 | Planning for Contingencies | Chapter 3 | W02 |
| 5 | Information Security Policy | Chapter 4 | |
| 6 | Developing the Security Program | Chapter 5 | W03 |
| 7 | Security Management Models | Chapter 6 | |
| 8 | Security Management Practices | Chapter 7 | W04 |
| 9 | Risk Management: Identifying & Accessing Risk | Chapter 8 | |
| 10 | Risk Management: Controlling Risk | Chapter 9 | W05 |
| 11 | Protection Mechanisms | Chapter 10 | |
| 12 | Personnel and Security, Law and Ethics | Chap 11 & 12 | W06 |
| 13 | Subject Revision | | |

# Lectures and Workshop: Wollongong Campus



# Lectures and Workshop: Liverpool Campus



# Attendance Requirements

- A minimum attendance of 80% of all scheduled classes is required.

- Although there will be no formal attendance check during lectures and workshops, it is strongly recommended that students attend all the lectures and workshops.

# Assessments

| No. | Assessment Name | Assessment Weight | Mapping to Subject Learning Outcome | Task Due |
|---|---|---|---|---|
| 1 | Quiz | 5% | SLO1, SLO2 | Week beginning 24 Mar 2025 (In lecture in Session Week 4)<br>Final submission time: 7:30pm |
| 2 | Assignment | 15% | SLO1, SLO2 | 18 Apr 2025 (Friday in Session Week 7)<br>Final submission time: 11:30pm |
| 3 | Group Report | 30% | SLO3, SLO4, SLO5, SLO6, SLO1, SLO2 | 30 May 2025 (Friday in Session Week 12)<br>Final submission time: 11:30pm |
| 4 | Final Exam | 50% | SLO1, SLO2, SLO3, SLO4, SLO5, SLO6 | Examination period |

**Detailed information will be published on Moodle in due course.**

| Assessment 1 | | | |
|---|---|---|---|
| **Assessment Name** | Quiz | **Assessment Type** | Quiz |
| **Weighting** | 5% | | |
| **Subject Learning Outcomes Assessed** | SLO1, SLO2 | **Individual or Group Assessment** | Individual |
| **Assessment Due** | Week beginning 24 Mar 2025 (In lecture in Session Week 4)<br>Final submission time: 7:30pm | | |
| **Assessment Description and Criteria** | The quiz will be conducted on Moodle at the end of Week 4's lecture. It consists of 5 multiple-choice questions. | | |
| **Length / Duration** | 10 minutes | | |
| **Method of Submission** | Online via Moodle | | |
| **Return of Assessed Work** | The result will be available on Moodle after the quiz. | | |

| Assessment 2 | | | |
|---|---|---|---|
| **Assessment Name** | Assignment | **Assessment Type** | Assignment |
| **Weighting** | 15% | | |
| **Subject Learning Outcomes Assessed** | SLO1, SLO2 | **Individual or Group Assessment** | Individual |
| **Assessment Due** | 18 Apr 2025 (Friday in Session Week 7)<br>Final submission time: 11:30pm | | |
| **Assessment Description and Criteria** | An individual report to address a given topic | | |
| **Length / Duration** | 2000 -- 2500 words | | |
| **Method of Submission** | Online via Moodle | | |
| **Return of Assessed Work** | Mark and feedback will be provided on Moodle. | | |

| Assessment 3 | | | |
|---|---|---|---|
| **Assessment Name** | Group Report | **Assessment Type** | Report |
| **Weighting** | 30% | | |
| **Subject Learning Outcomes Assessed** | SLO3, SLO4, SLO5, SLO6, SLO1, SLO2 | **Individual or Group Assessment** | Group |
| **Assessment Due** | 30 May 2025 (Friday in Session Week 12)<br>Final submission time: 11:30pm | | |
| **Assessment Description and Criteria** | A group report to address a given case study | | |
| **Length / Duration** | 4500 -- 5000 words | | |
| **Method of Submission** | Online via Moodle | | |
| **Return of Assessed Work** | Mark and feedback will be provided on Moodle. | | |

- Students can form groups by themselves (independent of the tutorial groups). Each group can consist of up to 6 students.
- A group selection procedure will also be available on Moodle

| Assessment 4 | | | |
|---|---|---|---|
| **Assessment Name** | Final Exam | **Assessment Type** | Exam |
| **Weighting** | 50% | | |
| **Subject Learning Outcomes Assessed** | SLO1, SLO2, SLO3, SLO4, SLO5, SLO6 | **Individual or Group Assessment** | Individual |
| **Assessment Due** | Examination period | | |
| **Assessment Description and Criteria** | Knowledge about the lectures | | |
| **Length / Duration** | 3 hours | | |
| **Method of Submission** | To be announced. | | |
| **Return of Assessed Work** | Mark will be released on SOLS by the University. | | |

**Approved format of the final exam:**
**Face-to-face paper-based**

# Minimum Performance Requirements and Hurdle Assessments

**All assessment tasks must be submitted, and students must achieve a minimum mark of 40% on the final assessment task.**

Students who do not meet the minimum performance requirements, as specified for each assessment, will receive a

**TF (Technical Fail)**

grade for this subject, which will appear on your Academic Transcript.

# Late Submissions of Assessment Tasks and Penalties

- Assessed work must be submitted in by the date and time given. If an assessment is submitted late, it will be marked in the normal way, and a penalty will then be applied.
- In the absence of an approved request for Academic Consideration in the form of an extension, assessment tasks must be submitted in line with the assessment instructions.
- Work submitted after seven calendar days will not be marked and will be given a mark of 0.
- No assessment task can be handed in for a mark once the assessment task has been returned to students.
- Penalties accrue on each day that the assessment task is late, including Saturday, Sunday and public holidays.
- Assessments must still be submitted to meet minimum performance requirements even though no mark is to be awarded

# Extensions

Students requesting an extension of time to submit an assessment task, deferred exam or exemption of a compulsory attendance requirement, must apply using Academic Consideration through SOLS.

Students must apply before, or on the assessment/s due date and where evidence is required, students must provide evidence no later than three working days after the assessable item's due date for their request to be considered. For information on the Academic Consideration Policy, eligibility requirements and how to apply, see https://www.uow.edu.au/student/admin/academic-consideration/

# Deferred Exams

- Deferred Exams are for students who applied for Academic Consideration to request to postpone their exam, and had their application approved by their subject coordinator.

- More information about Supplementary or Deferred Exams:
  https://www.uow.edu.au/student/exams/supplementary-exams/

# Supplementary Assessment

- Supplementary assessment may be offered to students whose performance in this subject is close to that required to pass the subject, and are otherwise identified as meriting an offer of a supplementary assessment.

- For information about eligibility criteria and the form and timing of supplementary assessments see https://policies.uow.edu.au/document/view-current.php?id=96

# Key Characteristics of Information Security

# Communities of Interest

Organizations must realize that information security funding and planning decisions involve more than just technical managers, such as information security managers or members of the information security team. Altogether, they should involve three distinct groups of decision makers, or **communities of interest**:

- Managers and professionals in the field of information security
- Managers and professionals in the field of IT
- Managers and professionals from the rest of the organization

The three groups should engage in constructive debate to reach consensus on an overall plan to protect the organization's information assets.

# Communities of Interest


The communities of interest and the roles they fulfill:

- The **InfoSec community** protects the organization's information assets from the many threats they face.
- The **IT community** supports the business objectives of the organization by supplying and supporting IT that is appropriate to the organization's needs.
- The **general business community** articulates and communicates organizational policy and objectives and allocates resources to the other groups.

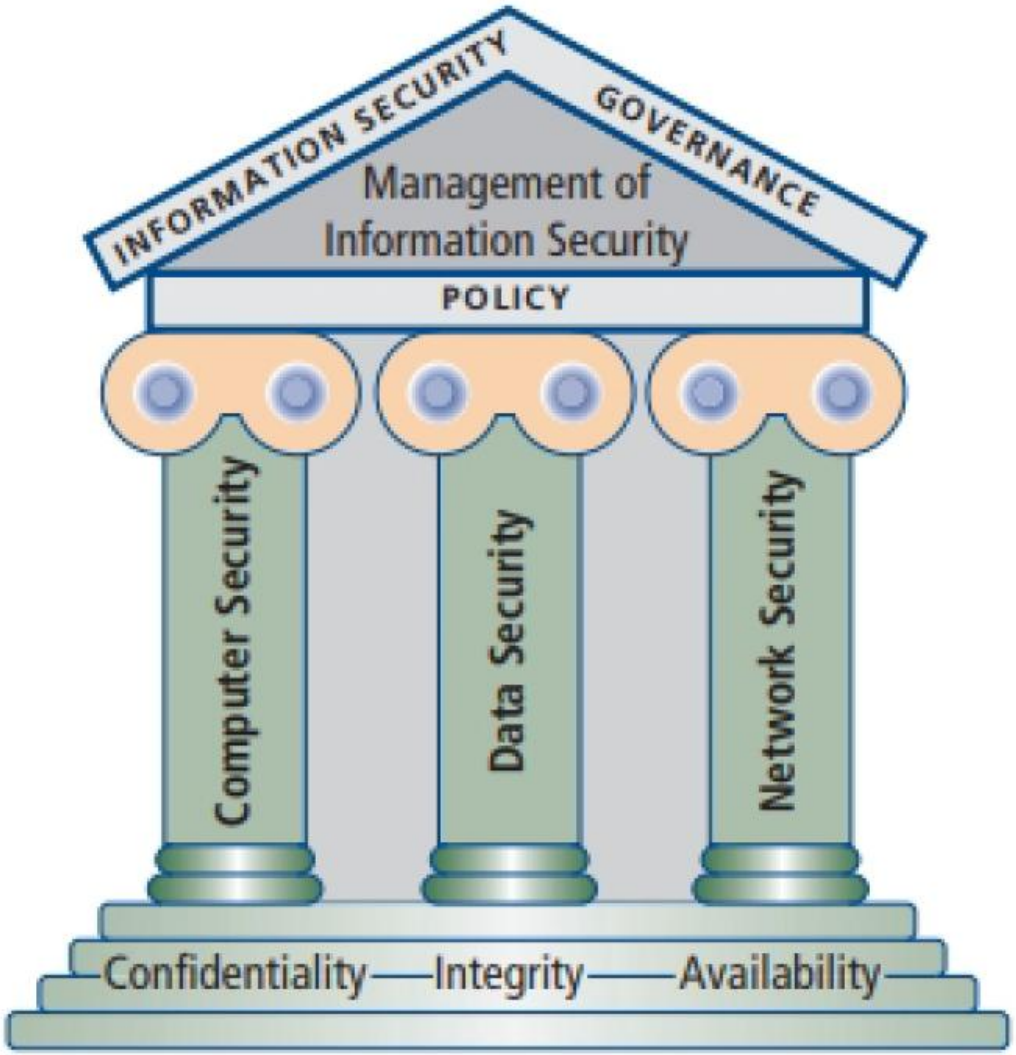
# What Is Security?

- Security is defined as “the quality or state of being secure—to be free from danger”
- Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another
- Specialized areas of security: Physical security, operations security, communications security, cyber security, and network security

# Information Security

- **Information Security (InfoSec):**
  - Often refers to the processes and tools which are designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.
  - Focuses on the protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information through a variety of protection mechanisms such as **policy**, **technology**, and **training and awareness programs**

# Components of Information Security

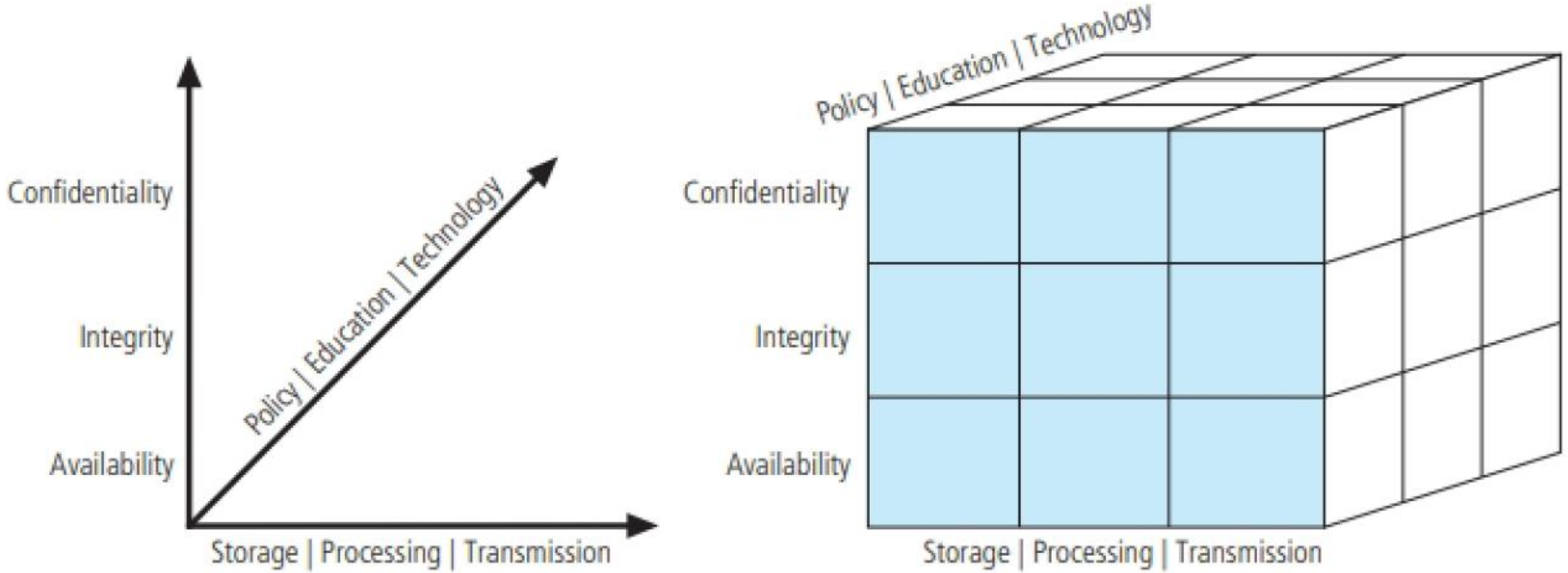


# CNSS Security Model

The Committee on National Security Systems (CNSS) document NSTISSI No. 4011, "National Training Standard for Information Systems Security (InfoSec) Professionals," presents a comprehensive model of InfoSec known as the McCumber Cube, which is named after its developer, John McCumber.

- Serves as the standard for understanding many aspects of InfoSec
- Covers the three dimensions that are central to information security: information characteristics, information location and security control categories.

# CNSS Security Model (cont'd.)




- Each cell represents an area of intersection among three dimensions that must be addressed to secure information systems.
- When using this model to design or review any information security program, you must make sure that each of the 27 cells is properly addressed by each of three communities of interest.

# CNSS Security Model (cont'd.)

- **Weaknesses of the CNSS Model**

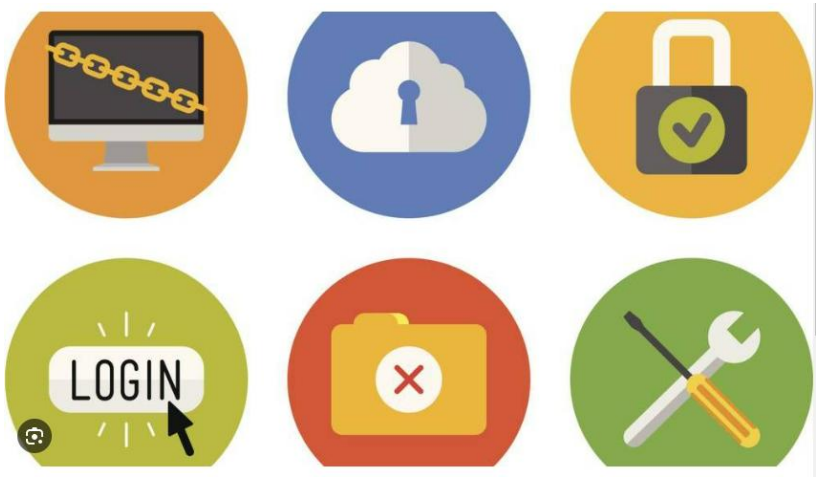
  - While the CNSS model covers the three dimensions of InfoSec, it omits any discussion of guidelines and policies that direct the implementation of controls, which are essential to an effective InfoSec program. Instead, the main purpose of the model is to identify gaps in the coverage of an InfoSec program.

  - Another weakness of this model emerges when it is viewed from a single perspective. In practice, thorough risk reduction requires the creation and dissemination of controls of all three types (policy, education, and technology) by all three communities.

# Key Concepts of Information Security

- **C.I.A. triangle**
  - Confidentiality, integrity, and availability
  - Has expanded into a more comprehensive list of critical characteristics of information: privacy, identification, authentication, authorization, accountability.

# Confidentiality




- **Confidentiality:** ensures that only those with sufficient privileges may access certain information
- Measures used to protect confidentiality
  - Information classification
  - Secure document (and data) storage
  - Application of general security policies
  - Education of information custodians and end users
  - Cryptography (encryption)

# Integrity

- **Integrity**

➢ The quality or state of being whole, complete, and uncorrupted.

➢ Information integrity is threatened if exposed to corruption, damage, destruction, or other disruption of its authentic state.

➢ Corruption can occur while information is being compiled, stored, or transmitted.

# Availability

- **Availability**
  - The characteristic of information that enables user access to information in a required format, without interference or obstruction
  - A user in this definition may be either a person or another computer system
  - Availability does not imply that the information is accessible to any user. It only implies availability to authorized users.

# Privacy

- **Privacy**
  - Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected.
  - Privacy as a characteristic of information does not signify freedom from observation. Information will be used only in ways known to the person who provided it.

# Identification

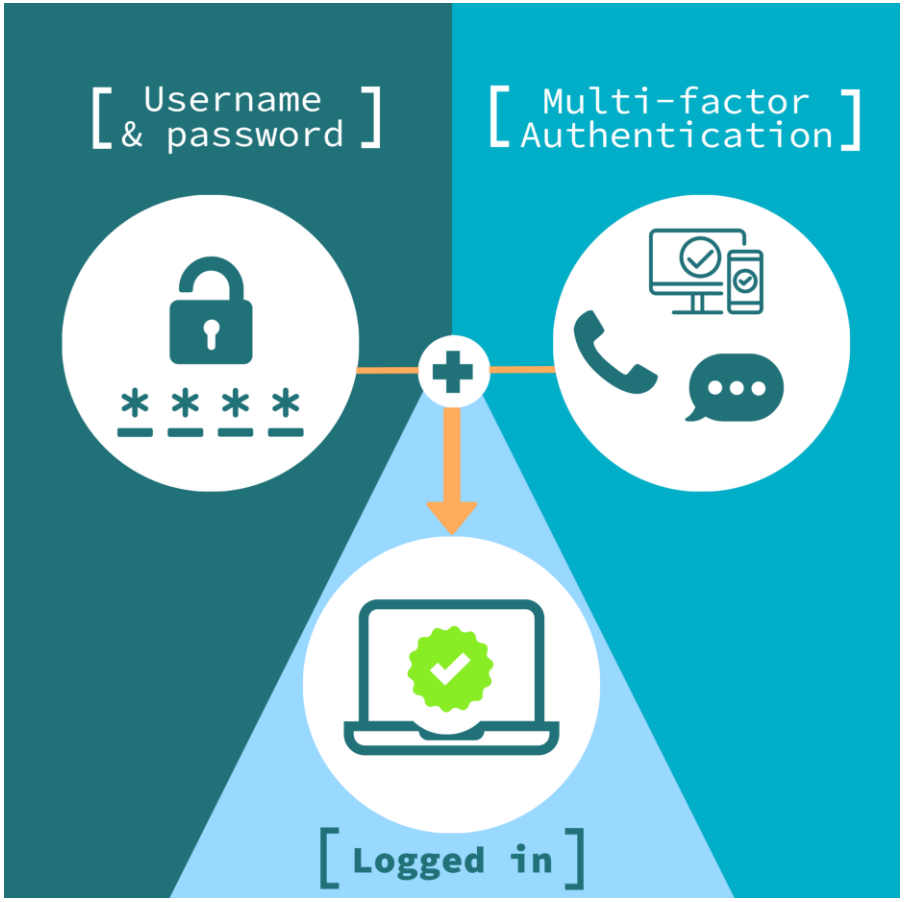
- **Identification**
  - An information system possesses the characteristic of identification when it is able to recognize individual users
  - First step in gaining access to secured material
  - Identification and authentication are essential to establishing the level of access or authorization that an individual is granted
  - Is typically performed by means of a username or other ID

# Authentication

- **Authentication**

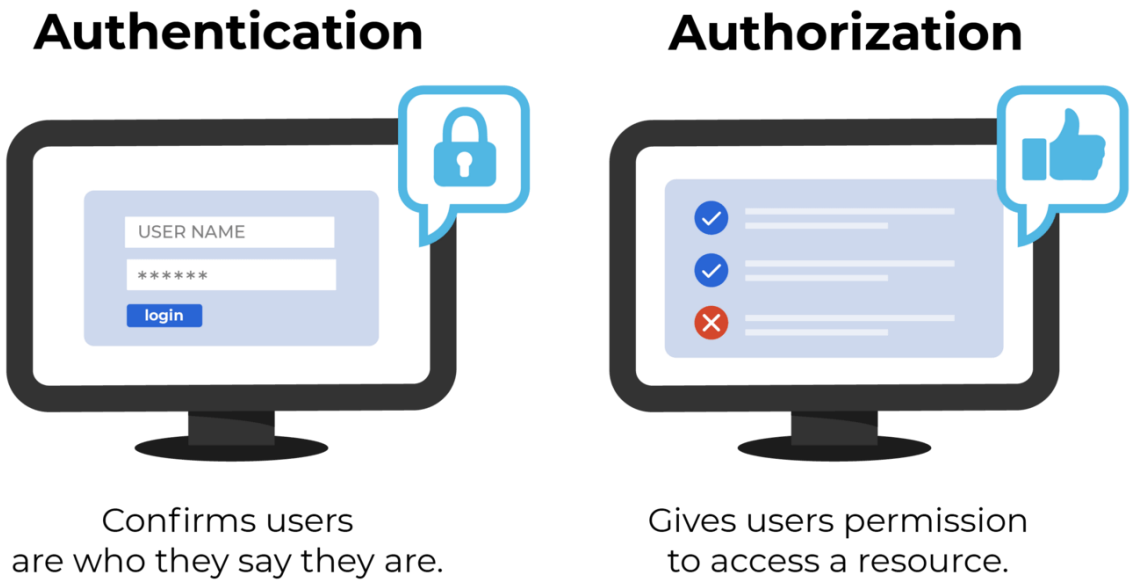
  - Occurs when a control proves that a user possesses the identity that he/she/it claims.

  - **Examples:** the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections, the use of cryptographic hardware



# Authorization

- **Authorization**
  - ➢ Authorization occurs after the identity of a user is authenticated
  - ➢ Assures that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset
  - ➢ User may be a person or a computer



# Accountability

- **Accountability**

  - Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process

  - Examples: audit logs (track user activity on an information system) provide accountability

# Homework Exercises

1. Distinguish **Confidentiality** and **Privacy**
2. Distinguish **Identification** and **Authentication**
3. Distinguish **Authentication** and **Authorization**
4. Are **Privacy** and **Accountability** contradicting concepts?

# What is Management?

# What Is Management?

- **Management:** The process of achieving objectives using a given set of resources.
- **Manager:** Someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals.
- **Managerial roles**
  - **Informational role:** Collecting, processing, and using information that can affect the completion of the objective.
  - **Interpersonal role:** Interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task.
  - **Decisional role:** Selecting from among alternative approaches, and resolving conflicts, dilemmas, or challenges.

# Leadership and Management

- There are differences between leadership and management.
- **Leadership:** The process of influencing others and gaining their willing cooperation to achieve an objective by providing purpose, direction, and motivation.
- A leader influences employees so that they are willing to accomplish objectives. A manager administers the resources of the organization.
- Behavioral types of leaders: autocratic, democratic and laissez-faire. Effective leaders typically function with a combination of these 3 styles, shifting approaches as situations warrant.