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 2024

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."

Overview of the Subject

Contact Details

Dr Khoa NGUYEN

- Office: 3.213
- Email: khoa@uow.edu.au
- Subject title starts with [CSIT988]
- Consultation hours:
  - Tuesday 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
  - Discussion forums
  - Polls, quizzes
  - Assessment details
- Students should regularly check the subject's Moodle site https://moodle.uowplatform.edu.au/course/view.php?id=39388,

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

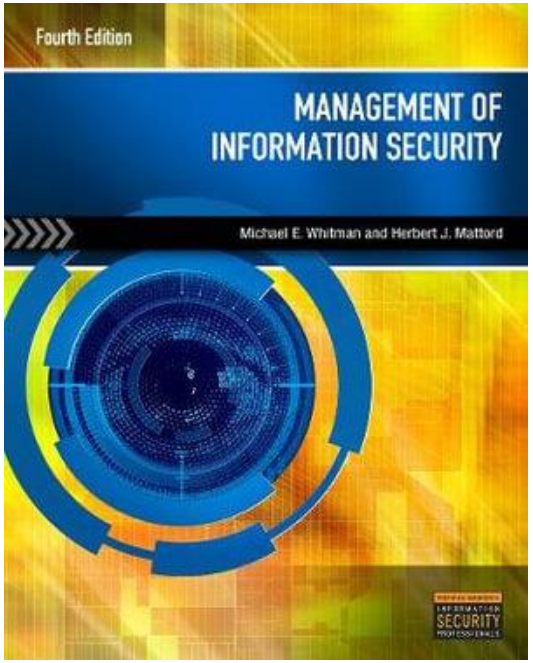
1. Apply the security system development life cycle to create a comprehensive security posture.
2. Implement effective information security planning, including contingency planning.
3. Analyse emerging trends in information security management practices.
4. Implement information security planning against 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.

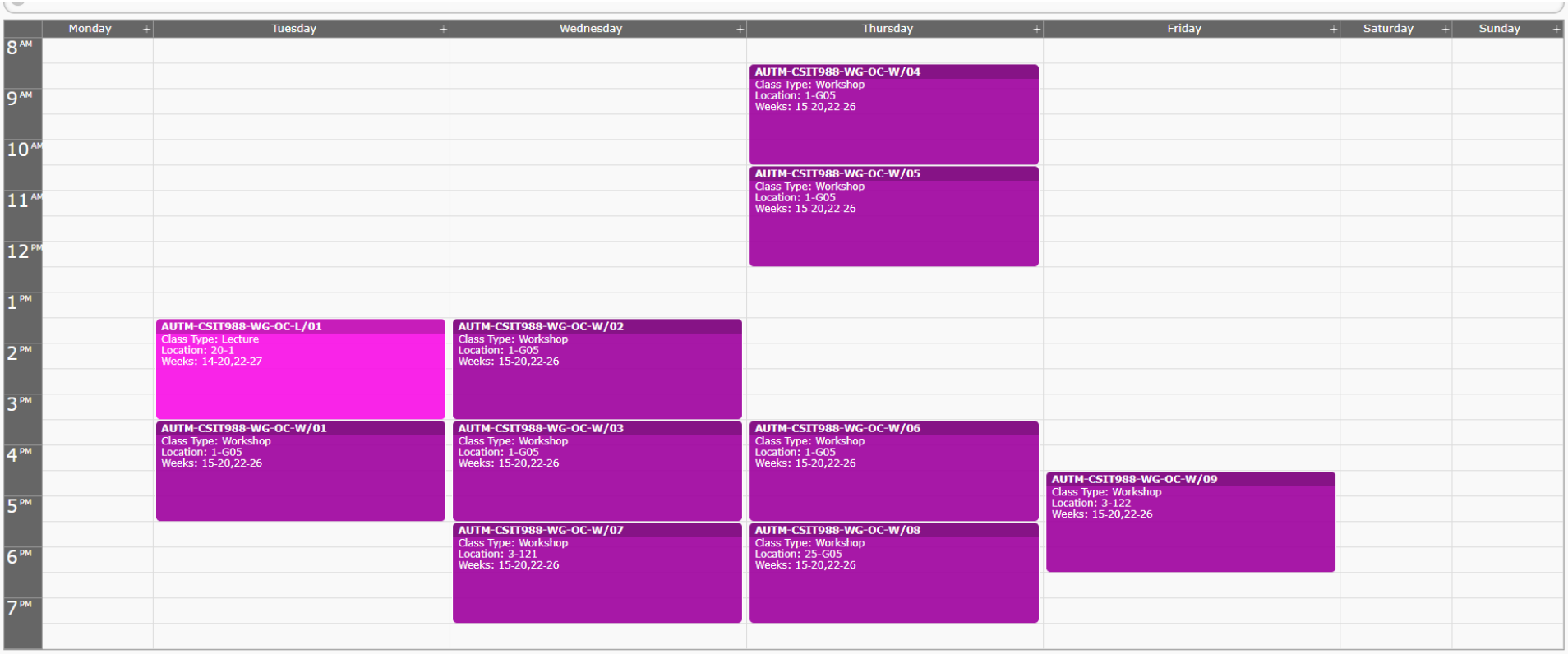
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, **Security in Computing**, 5th Edition, Pearson, 2015.

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

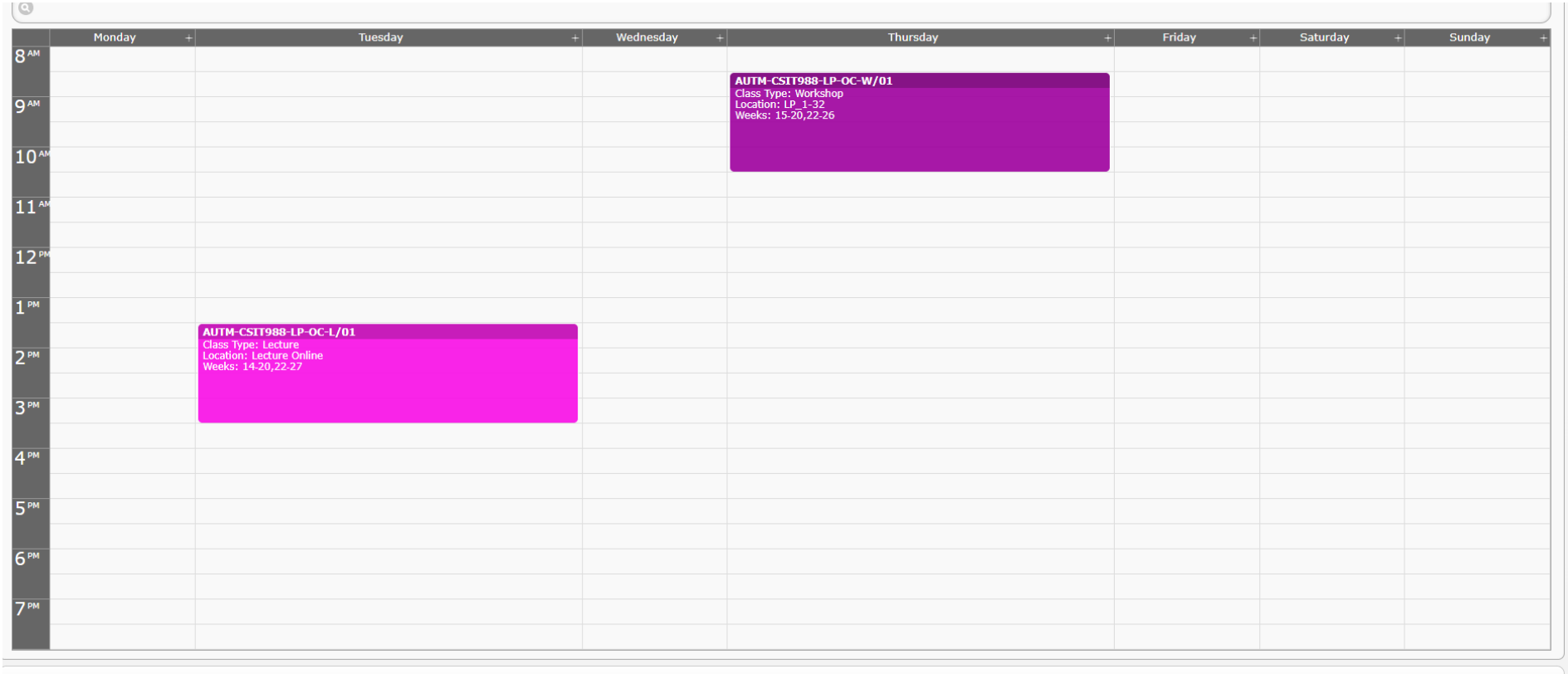
- **The Cyber Security Body of Knowledge**, Version 1.1.0, The National Cyber Security Centre, 2021. Available at https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Week	Lecture Topic(s)	Reading(s)	Workshop
1	Introduction and Overview of the Subject	**SO + Chapter 1**	**No**
2	Information Security Management	Chapter 1	W01
3	Planning for Security	Chapter 2	W02
4	Planning for Contingencies	Chapter 3	W03
5	Information Security Policy	Chapter 4	W04
6	Developing the Security Program	Chapter 5	W05
7	Security Management Models	Chapter 6	W06
8	Security Management Practices	Chapter 7	W07
9	Risk Management: Identifying & Accessing Risk	Chapter 8	W08
10	Risk Management: Controlling Risk	Chapter 9	W09
11	Protection Mechanisms	Chapter 10	W10
12	Personnel and Security, Law and Ethics	Chap 11 & 12	W11
13	Subject Review		No

Lectures and Workshop: Wollongong Campus



Lectures and Workshop: Liverpool Campus



Workshop demonstrators

Four qualified demonstrators (one PhD holder and three PhD candidates in SCIT) will help run the workshops.

- **Dr Thanh NGUYEN,** thanhngocn@uow.edu.au (Liverpool W/01)
- **Ms Mei JIANG,** mjiang@uow.edu.au (Wollongong W/02, W/03, W/07)
- **Ms Wenchao LI,** wenchaoli@uow.edu.au (Wollongong, W/04, W/05)
- **Mr Danh Nam TRAN**, danht@uow.edu.au (Wollongong, W/06, W/08, W/09)

Wollongong W/01 will be run by me (Dr Khoa Nguyen).

Assessments

No.	Assessment Name	Assessment Weight	Mapping to Subject Learning Outcome	Task Due
1	Report	10%	SLO1, SLO2	22 Mar 2024 (Friday in Session Week 4) Final submission time: 11:30pm
2	Presentation	10%	SLO1, SLO2	14 Apr 2024 (Sunday in Session Week 7) Final submission time: 11:30pm
3	Report	30%	SLO3, SLO4, SLO5, SLO6, SLO1, SLO2	22 May 2024 (Wednesday in Session Week 12) 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	Report	**Assessment Type**	Report
Weighting	10%		
Subject Learning Outcomes Assessed	SLO1, SLO2	**Individual or Group Assessment**	Individual
Assessment Due	22 Mar 2024 (Friday in Session Week 4) Final submission time: 11:30pm		
Assessment Description and Criteria	Individual report to address the given topic		
Length / Duration	2000 -- 2500 words		
Method of Submission	Online via Moodle		
Return of Assessed Work	Grade and feedback will be provided on Moodle.		

Assessment 2			
Assessment Name	Presentation	**Assessment Type**	Presentation
Weighting	10%		
Subject Learning Outcomes Assessed	SLO1, SLO2	**Individual or Group Assessment**	Individual
Assessment Due	14 Apr 2024 (Sunday in Session Week 7) Final submission time: 11:30pm		
Assessment Description and Criteria	Content and presentation skills		
Length / Duration	10 minutes		
Method of Submission	Online via Moodle		
Return of Assessed Work	Grade and feedback will be provided on Moodle.		

Assessment 3			
Assessment Name	Report	**Assessment Type**	Report
Weighting	30%		
Subject Learning Outcomes Assessed	SLO3, SLO4, SLO5, SLO6, SLO1, SLO2	**Individual or Group Assessment**	Group
Assessment Due	22 May 2024 (Wednesday in Session Week 12) Final submission time: 11:30pm		
Assessment Description and Criteria	Group report to address the given case study		
Length / Duration	4500 -- 5000 words		
Method of Submission	Online via Moodle		
Return of Assessed Work	Grade 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	Marks will be released on SOLS by the University.		

Technical Fail

To be eligible for a Pass in this subject a **student must achieve a mark of at least 40% in the Final Exam**.

Students who fail to achieve this minimum mark and would have otherwise passed may be given a **TF (Technical Fail)**

for this subject, which will appear on their Academic Transcript.

Late Submissions and Penalties

- Penalties apply to all late work, except if student academic consideration has been granted.
- Late submissions will attract a penalty of 25% of the assessment mark per day. Work more than 4 days late will be awarded a mark of zero.
- If an assessment is submitted late, it will be marked in the normal way, and a penalty will then be applied.
- Submissions received 15 days after the due date will receive no feedback. However, lecturers may choose to provide feedback at their discretion.

Supplementary Exams

- The School does not normally offer a supplementary exam to a student who has sat a scheduled exam.
- Supplementary Exams will be dealt with in accordance with student academic consideration policy.
- While the School normally grants supplementary exams when the student does not sit the standard exam for an acceptable reason, each case will be assessed on its own merit and there is no guarantee a supplementary exam will be granted.
- If a supplementary exam is granted, you will normally be notified via SOLS Mail about the time and date of this supplementary exam. You must follow the instructions given in the email message.
- Please note that if this is your last session and you are granted a supplementary exam, be aware that your results will not be processed in time to meet the graduation deadline.

Attendance Requirements

- It is the responsibility of students to attend all lectures/workshops for subjects for which you are enrolled. It should be noted that the amount of time spent on each 6-credit-point subject should be at least 12 hours per week, which includes lectures, personal studies, writing reports, etc.

- Satisfactory attendance is deemed by the University, to be attendance at approximately 80% of the allocated contact hours.

- In order to maximize learning outcomes, **it is strongly recommended that students attend all the lectures and workshops**.

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.

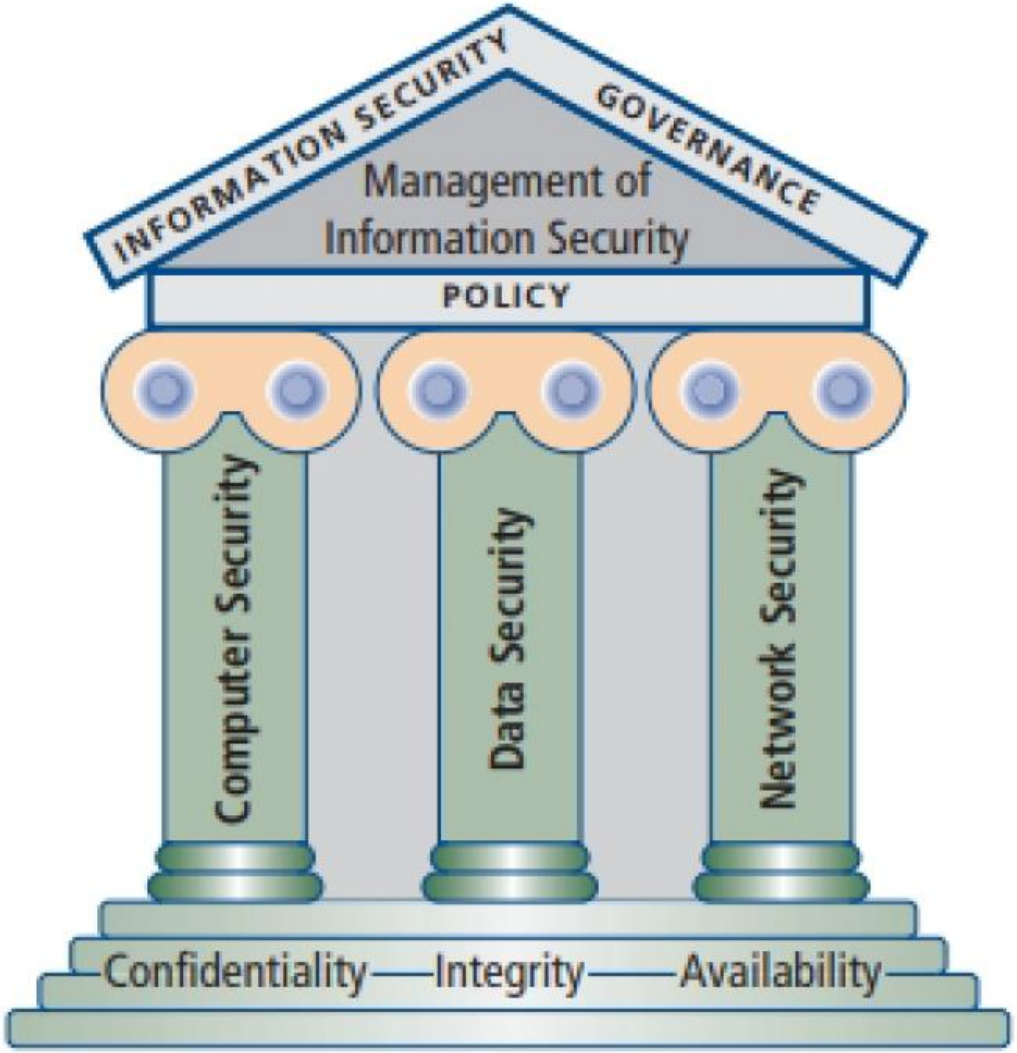
What Is Security?

- 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

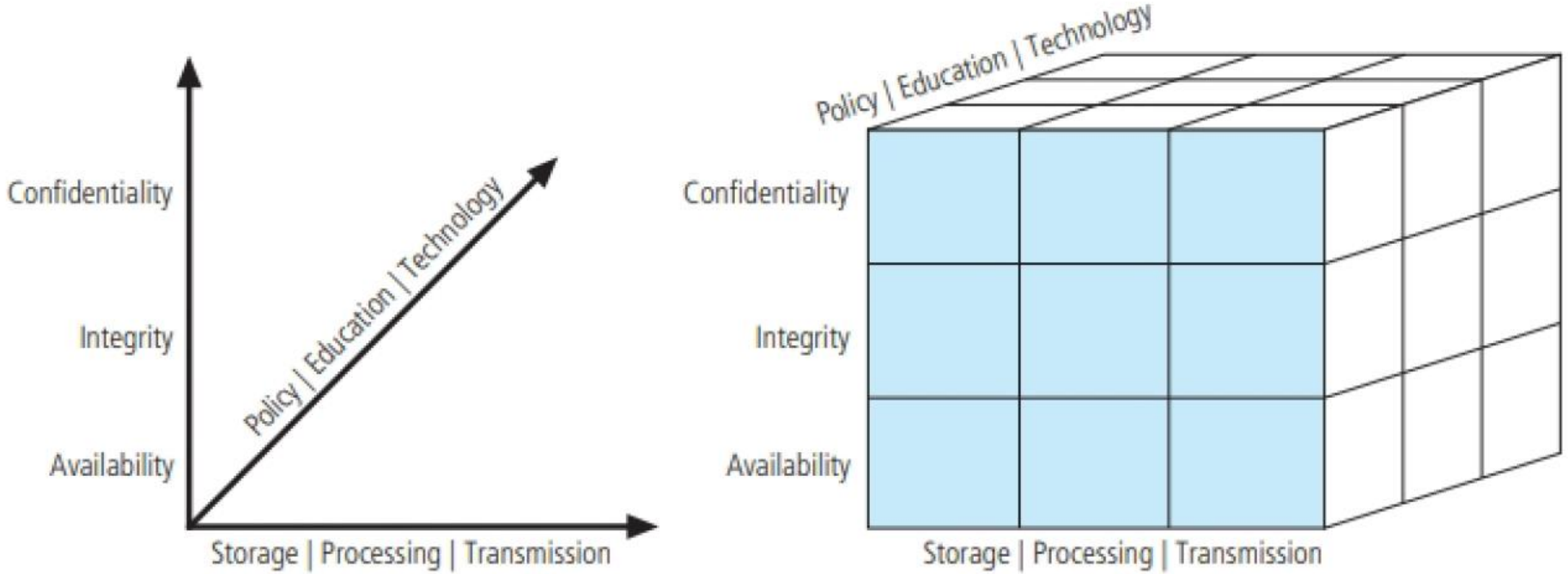


CNSS Security Model

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**

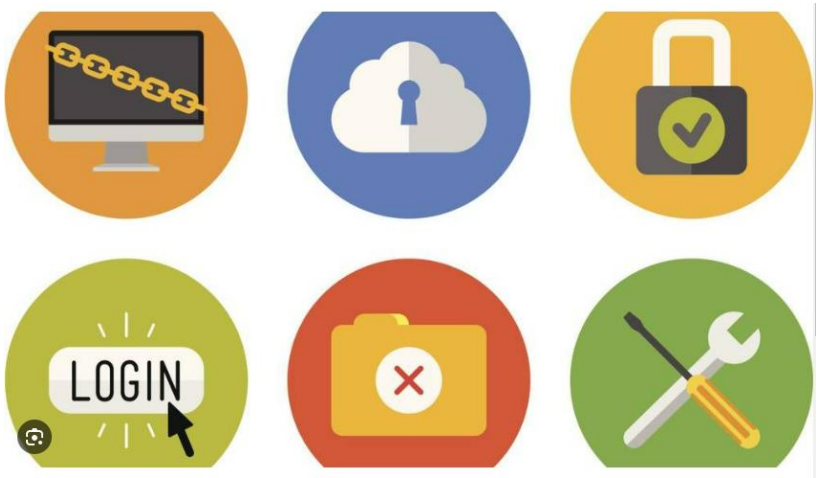
  - While the CNSS model covers the three dimensions of InfoSec, it omits any discussion of guidelines and policies that direct the implementation of controls, which are essential to an effective InfoSec program. Instead, the main purpose of the model is to identify gaps in the coverage of an InfoSec program.

  - 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

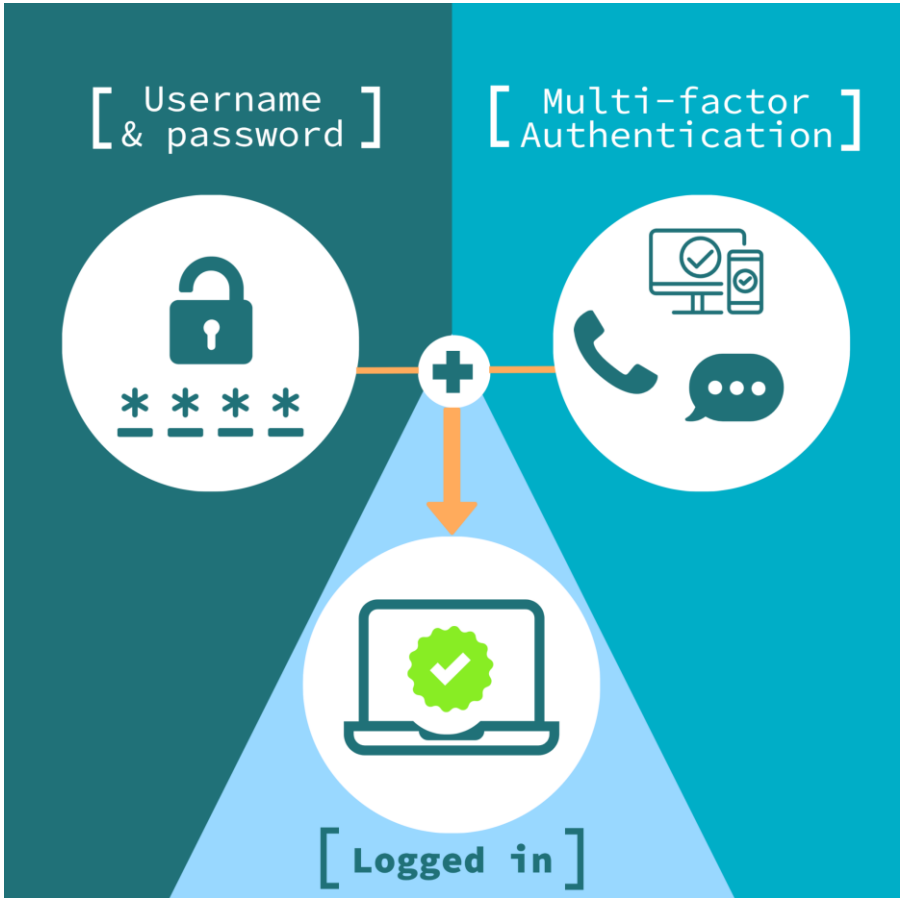
- **Privacy**
  - Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected.
  - Privacy as a characteristic of information does not signify freedom from observation. Information will be used only in ways known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

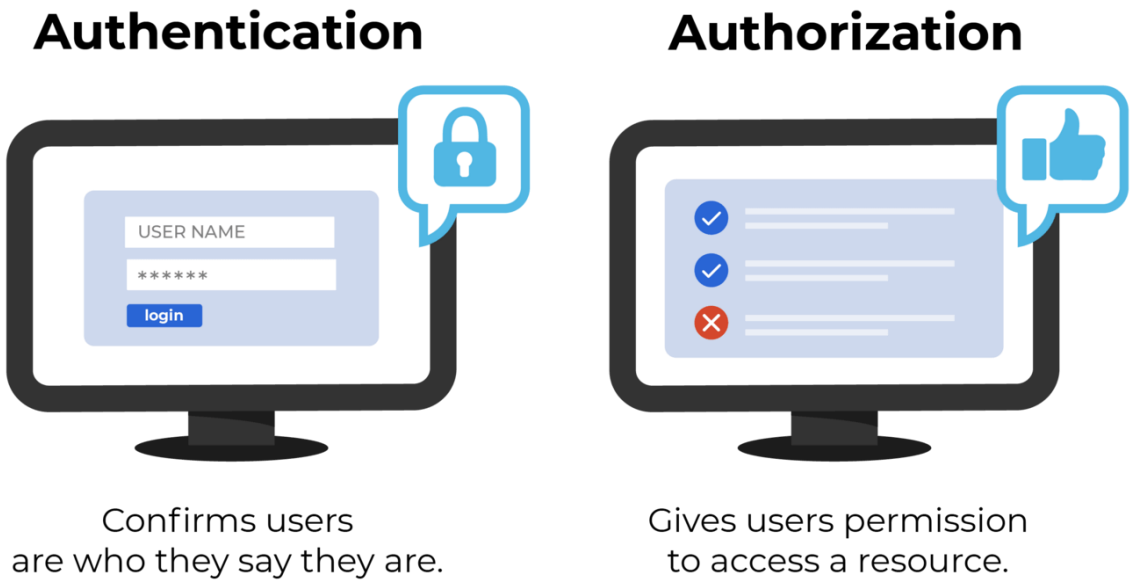
Authentication

- **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.