CSIT988/CSIT488
Security, Ethics and Professionalism
Week 13: Subject Revision

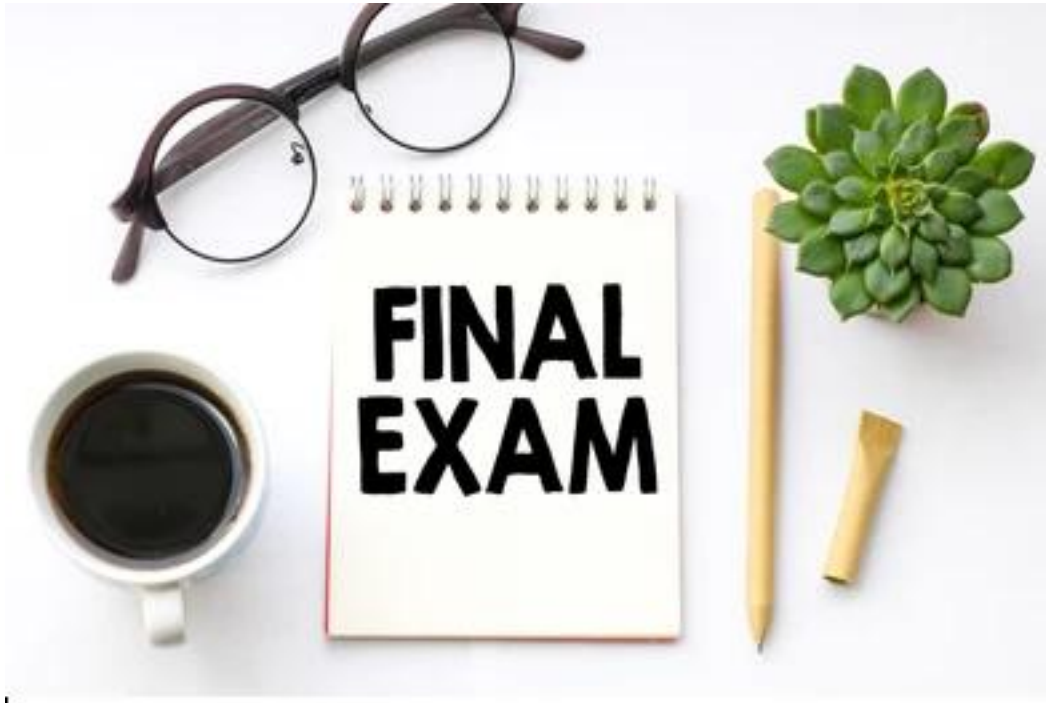
Subject Coordinator: Dr Khoa Nguyen

School of Computing and Information Technology

Autumn 2025

Roadmap

- **Subject Revision**
  - ➢ **Key Concepts**
  - ➢**The Final Exam**
  - ➢ **Q & A**



shutterstock.com · 1681582195

Key Concepts

Basics of Information Security

- What is information security?
- Communities of interest: InfoSec, IT, general business
- The CNSS security model and its three dimensions
- C.I.A triangle: confidentiality, integrity, availability
- Privacy, identification, authentication, authorisation, accountability

InfoSec Management

- What is management?
- POLC principles: Planning, Organizing, Leading, Controlling
- The six P’s of InfoSec management: Planning, Policy, Programs, Protection, People, Projects
- PMBoK (Project Management Body of Knowledge) knowledge areas: Integration, Scope, Time, Cost, Quality, Human resource, Communications, Risk, Procurement
- Project Management tools: Work Breakdown Structure (WBS), Program Evaluation and Review Technique (PERT), Gantt Charts
- Critical path, Slack time

Planning for Security

- What is planning?
- Foundational documents: Values statement, Vision statement, Mission statement
- Strategic planning: creating a strategic plan, planning levels, planning and the CISO
- The IDEAL model governance framework: Initiating, Diagnosing, Establishing, Acting, and Learning
- Planning for InfoSec implementation
  - ➢ Bottom-up approach vs Top-down approach
- SecSDLC (Security Systems Development Life Cycle):
  - ➢ Waterfall methodology: Investigation, Analysis, Logical Design, Physical Design, Implementation, Maintenance and Change.
- Threats to InfoSec, attacks, vulnerabilities, etc.

Planning for Contingencies

- Fundamentals of contingency planning (CP)
  - What is CP? Why is it important?

- Components of CP: Business impact analysis (BIA), Incident response plan (IR plan), Disaster recovery plan (DR plan), Business continuity plan (BC plan)

- For each component: Why is it important? What are the major concepts?

InfoSec Policy

- Why policy?
  - Bull’s-eye model: Policies, Networks, Systems, Applications

- Types of information security policy:
  - Enterprise information security program policy (EISP)
  - Issue-specific information security policies (ISSP)
  - Systems-specific policies (SysSP)

- Goals, components, implementations for each of EISP, ISSP, SysSP
- Guidelines for effective policy: development, distribution, review, comprehension (understanding), compliance (agreement), and uniform enforcement

Developing the Security Program

- Organizing for security
  - Variables involved in structuring an InfoSec program
  - Functions needed to implement the InfoSec program
  - Security in large, medium-size and small organizations

- Placing InfoSec within an organization:
  - Charles Wood’s five options on InfoSec program positioning
  - Other options
  - Advantages and limitations of each reporting structure

- InfoSec roles and titles: CISO, security managers, security administrators and analysts, security technicians, security consultants, security officers and investigators, etc.
- SETA (security education, training, and awareness) programs: purpose, benefits, effective implementations

Security Management Models

- Blueprints, frameworks, security models
- Access control models
  - ➢ Definitions of access control
  - ➢ Essential processes (identification, authentication, authorization, accountability),
  - ➢ Key principles (least privilege, need-to-know, separation of duties)
  - ➢ Categories of access control: Based on inherent characteristics, Based on operational impact, Based on the degree of authority
  - ➢ Data classification models, Security clearances

- Security architecture models: Trusted Computing Base, Information Technology System Evaluation Criteria, The Common Criteria
- The Bell-LaPadula Confidentiality Model & the BiBa Integrity Model
- Security management models: ISO 27000 series, NIST Security Models

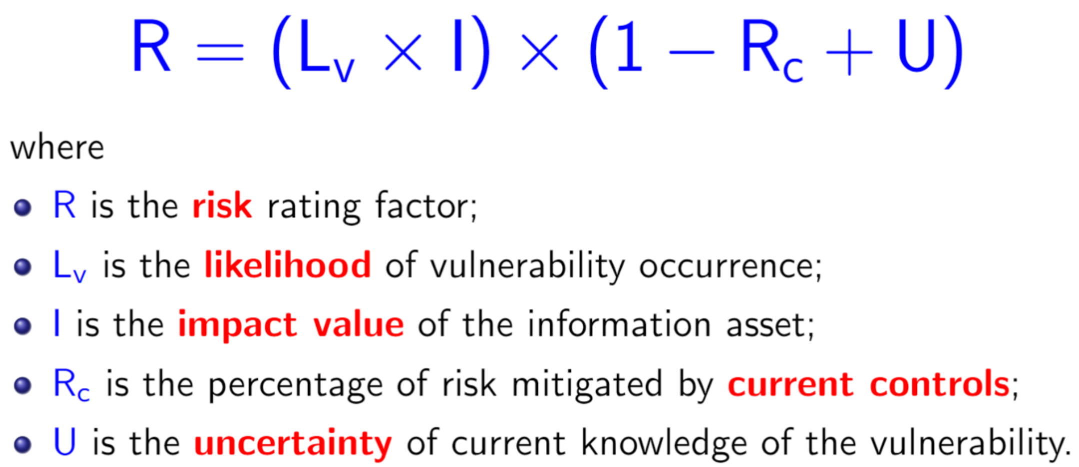
Security Management Practices

- Benchmarking: goals, categories (standards of due care/due diligence, best practices), selecting recommended practices, limitations
- Baselining, supports for baselining and recommended practices
- Performance measurement in InfoSec management: definitions, types, critical factors to the success of InfoSec performance programs
- Trends in certification and accreditation

Risk Management: Identifying and Assessing Risks

- What is risk management? What are its key areas of concern? Who should be responsible? Who should take the lead?
- Risk identification: goal and importance, main tasks
  - ➢ TVA worksheet

- Risk assessment: goals, concepts, formulas for calculating risks, possible controls, documenting
  - ➢ Likelihood, value of information asset, current controls, uncertainty



$$R = (L_v \times I) \times (1 - R_c + U)$$

where

- R is the **risk** rating factor;
- L_v is the **likelihood** of vulnerability occurrence;
- I is the **impact value** of the information asset;
- R_c is the percentage of risk mitigated by **current controls**;
- U is the **uncertainty** of current knowledge of the vulnerability.

Risk Management: Controlling Risks

- Risk control strategies: defense, transference, mitigation, acceptance, termination
- Managing risks: Risk appetite, Residual risk, Guidelines for risk control strategy selection

- **Cost-Benefit Analysis (CBA)**
  - Economic feasibility, cost, benefit, assess valuation, potential loss
  - Assess value (AV), Exposure factor (EF), Annualized loss expectancy (ALE), single loss expectancy (SLE), annualized rate of occurrence (ARO),
  - **SLE = asset value (AV) x exposure factor (EF)**
  - **ALE = SLE * ARO**
  - **CBA = ALE(prior) – ALE(post) – ACS**

Protection Mechanisms

- Four processes of access control: identification, authentication, authorization, accountability
- **Firewalls**: the development of firewalls (1st, 2nd, 3rd and 4th generations), firewall architectures
- **IDPSs**: types (host-based and network-based) and detection methods (signature-based and anomaly-based)
- **Cryptography**:
  - ➢ Components of cryptology (cryptography, cryptanalysis)
  - ➢ Encryption, decryption, key, key space, plaintext, ciphertext
  - ➢ Symmetric encryption vs asymmetric encryption
  - ➢ Digital certificates, PKI, hybrid cryptosystems
  - ➢ Notable cryptographic protocols

Personnel and Security, Laws and Ethics

- Staffing the security function:
  - InfoSec positions: those who define, those who build, those who administer; CISO, managers, administrators, technicians, etc.
  - Qualifications and requirements
- InfoSec professional credentials: CISSP, SSCP
- Employment policies and practices:
  - Hiring: interview, orientation, training, check, contract
  - Firing: hostile vs friendly departures
  - Methods of monitoring and controlling employee
  - Security considerations for non-employees
- Laws and Ethics
  - Laws, policies, ethics – similarity and difference
  - InfoSec laws: US, international, Australia

The Final Exam

Assessments

Assessment	%	Type	Date
1. **Assignment 1:** Quiz	5	Individual	DONE
2. **Assignment 2:** Report	15	Individual	DONE
3. **Assignment 3:** Group Report	30	Group	DONE
4. **Final Exam**	50	Individual	**Monday, 16 June, 2025, 09:00am – 12:00pm**

Technical Fail

- To be eligible for a Pass in this subject a student must achieve a mark of at least **40% (20 out of 50)** in the Final Exam.

- Students who fail to achieve this minimum mark & would have otherwise passed may be given a TF (Technical Fail) for this subject.

Final Exam: Restrictions

The exam is

- **Paper-based, venue specified in you timetable**
- **RESTRICTED - only specified reference materials permitted.**

You may bring:

- **10 A4 pages of hand-written or printed notes.**
  - ✓ **No restriction on what are written/printed on the 10 A4 pages.**

- **UOW Approved Calculator**

Final Exam: Question Structure

Total marks: 50

- **10 MCQ questions (2 marks each)**
- **10 short-answer questions (2 marks each)**
- **1 case study question (2 sub-questions, 5 marks each)**

Final Exam: MCQ Questions

- Each question has 5 choices
- The number of correct choices could be either 1, or 2 or 3.
- Mark deductions applied for incorrect choices.
- If there are X (1 ≤ X ≤ 3) correct answers
  - For each correct choice: **+100/X %** of the mark
  - For each incorrect choice: **-100/(5-X) %** of the mark
- **For each question, the mark you can get is at least 0 and at most 2. That is the mark is never negative and you should attempt to answer all questions.**

Examples of MCQ Questions

Which of the following statements are true?

Select one or more:

A. It is extremely uncommon for a CISO to have a CISSP.

B. InfoSec consideration should be part of the hiring process.

C. A background check should be conducted before the organization extends an offer to any security technician.

D. Job rotation is based on the principle of least privilege.

E. Ethics are rules adopted and enforced by governments.

Examples of MCQ Questions

Which of the following statements are true?

Select one or more:

A. It is extremely uncommon for a CISO to have a CISSP. **(-33.33%)**

B. InfoSec consideration should be part of the hiring process. **(+50%)**

C. A background check should be conducted before the organization extends an offer to any security technician. **(+50%)**

D. Job rotation is based on the principle of least privilege. **(-33.33%)**

E. Ethics are rules adopted and enforced by governments. **(-33.33%)**

Examples of MCQ Questions

Which of the following statements are true?

Select one or more:

A. The BiBa integrity model is based on the principle of "no read up, no write down".

B. Asymmetric encryption systems are usually less efficient than symmetric encryption systems.

C. The values statement describes what an organization wants to become.

D. Risk analysis is a major component of risk management.

E. An example of technical attack to InfoSec is shoulder surfing.

Examples of MCQ Questions

Which of the following statements are true?

Select one or more:

A. The BiBa integrity model is based on the principle of "no read up, no write down". **(-25%)**

B. Asymmetric encryption systems are usually less efficient than symmetric encryption systems. **(+100%)**

C. The values statement describes what an organization wants to become. **(-25%)**

D. Risk management is a major component of risk analysis. **(-25%)**

E. An example of technical attack to InfoSec is shoulder surfing. **(-25%)**

Final Exam: Short-Answer Questions

- Similar to the short-answer questions in the workshops

- **Example:** *What is access control? What are the essential processes of access control? What are the key principles on which access control is founded?*

- There could be question(s) involving simple calculations.

Final Exam: Case Study

- You are given a case in InfoSec management.
    - ➢ Similar to the case of Hillside hospital in Assignment 3.

- You are asked to answer **two questions** regarding the case.
    - ➢ 5 marks for each question.

Some Advices for the Final Exam

- Study the textbook, lecture notes and workshop materials
- Prepare the notes! (Up to 10 A4 pages)
- Attempt to answer ALL questions

GOOD LUCK!

Your questions?