管院學士班課程大綱
BA/BBA Program Syllabus

系所 Department	資管所 IM	必選修 compulsory/elective	選修 Elective
課程名稱 Course title	Information Security (資訊安全技術)	學分數 Credit(s)	3
課號 Course Code		全英文授課 English Taught (EMI)	是(Yes)
學年/學期 academic year/Semester	115/01	上課地點 Classroom	MA221
講授教師 Instructor	Kankham Sarawut (沙拉溫)	上課時間 Time	Monday and Wednesday: 8:45 to 10:00
教師辦公室&諮詢時間 Instructor office & office hour	By appointment (Room 621)	教師聯絡資訊 Instructor Contact	Phone: 05-2720411#34604 Email: bensarawut@ccu.edu.tw
助教 Teaching assistant		助教 聯絡資訊 TA contact	Email:
先修課程 Pre-requisite courses	- Introduction to Information Management (Essential) - Network Management (Optional)		
學習目標 Learning Objective	• Understand core information security concepts, including the CIA triad, common threats, and basic protection mechanisms. • Analyze security risks, vulnerabilities, and their impact on individuals and organizations. • Apply information security principles and best practices to address real-world cybersecurity issues. • Develop foundational knowledge aligned with the core domains of the ISC2 Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) to support advanced studies, professional certification, and careers in cybersecurity and information security management.		
課程概述 Course Descriptions	This course introduces the fundamental concepts, principles, and selected technical approaches of information security, with a focus on protecting organizational and personal information in digital environments. Undergraduate students will learn essential topics, including the CIA triad, common cyber threats, vulnerabilities, risk management, security governance, access control, cryptography, network security, incident response, and security maintenance.		

<table>
<tr><td></td><td colspan="4">The course emphasizes practical applications through security policies, risk assessment, protection strategies, and the analysis of real-world cybersecurity incidents. In addition, the course content is aligned with the core knowledge domains of the ISC2 Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK), providing students with a strong academic foundation for advanced studies and future professional certification while developing the foundational knowledge and skills required for careers in cybersecurity, information security management, and related fields.</td></tr>
<tr><td colspan="5">對應 AOL 職能素養(AOL Competency)</td></tr>
<tr><td colspan="2">職能素養 4(Competency 4): 全球視野 Global Perspective</td><td colspan="3">職能素養 1(Competency 1): 知識整合 Knowledge Integration</td></tr>
<tr><td>課程類別
Course Attributes</td><td colspan="4">□人文關懷課程(Humanities Caring) □競賽專題課程(Competition)
☒問題導向課程(Problem-solving) □專題導向課程(Project-based)
☒實作課程(Practice-based) ☒總整課程(Capstone)</td></tr>
<tr><td>教材編選
Teaching materials</td><td colspan="4">☒自製簡報(self-made PPTs) □課程講義(Teaching Notes)
□自編教科書(self-made textbooks) □教學程式(programming)
□自製教學影片(self-made video) □其他(Others)</td></tr>
<tr><td>教學資源
Teaching Resources</td><td colspan="4">□課程網站(Website) □實習網站(Intern Web)
☒教材電子檔供下載(Downloadable Files)</td></tr>
<tr><td>教科書/參考書
Textbooks/References</td><td colspan="4"><u>Main Textbook</u>
• Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th ed.). Cengage.
<u>Supplementary Books</u>
• General Cybersecurity
  • Steinberg, J. (2025). Cybersecurity for dummies (3rd ed.). Wiley.
• Professional Certification (CISSP)
  • Miller, L. C., & Gregory, P. H. (2024). CISSP for dummies (8th ed.). Wiley.
  • Chapple, M., Stewart, J. M., & Gibson, D. (2024). ISC2 CISSP certified information systems security professional official study guide (10th ed.). Sybex.
• Supplementary Practice Resources (Optional)
  • Chapple, M., Stewart, J. M., & Gibson, D. (2024). ISC2 CISSP official practice tests (4th ed.). Sybex.</td></tr>
<tr><td rowspan="6">評量方式(請填百分比)
Assessment</td><td>課堂參與 Participation</td><td>15%</td><td>個案討論 Case study</td><td>%</td></tr>
<tr><td>作業 Homework</td><td>%</td><td>專題 Project</td><td>30%</td></tr>
<tr><td>小考 Quiz</td><td>%</td><td>其他 1 other ( )</td><td>%</td></tr>
<tr><td>期中考 Midterm Exam</td><td>%</td><td>其他 2 other ( )</td><td>%</td></tr>
<tr><td>期末考 Final Exam</td><td>30%</td><td>其他 3 other ( )</td><td>%</td></tr>
<tr><td>報告 Presentation</td><td>25%</td><td>其他 4 other ( )</td><td>%</td></tr>
</table>

其他說明 Other description	• The instructor reserves the right to make changes to this syllabus, such as class schedule, grading policy, etc., if necessary. • Undergraduate students must use credible and properly cited sources throughout both the Midterm Presentation and the Final Presentation. AI tools may be used to support learning; however, students are responsible for verifying all information and references. AI hallucinations and fabricated or inaccurate AI-generated references are strictly prohibited. All content must reflect the group's own understanding and critical analysis.

課程規劃表 Course Schedule

週次 **week**	日期 **Date**	內容 **Description**	教材章節 **Textbook**		其他說明 **Remark**
			Principles of Information Security	CISSP Domain	
1.		Course Overview	-	-	
2.		Course Introduction & Cybersecurity Landscape	Module 1	Domain 1	Assign Midterm Presentation
3.		The Need for Security	Module 2	Domain 1	
4.		Information Security Management	Module 3	Domain 1	
5.		Risk Management	Module 4	Domain 1	
6.		Incident Response & Business Continuity	Module 5	Domain 7	
7.		Legal, Ethical, and Professional Issues	Module 6	Domain 1	
8.		Security and Personnel	Module 7	Domain 1 & 5	
9.		**Midterm Presentation: Real-World Cybersecurity Case Analysis**	-	Integrated	
10		Security Technology: Access Controls, Firewalls, and VPNs	Module 8	Domain 3-5	Assign Final Presentation
11.		Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools	Module 9	Domain 4, 6 & 7	
12.		Cryptography	Module 10	Domain 3	
13.		Implementing Information Security	Module 11	Domain 7	
14.		Information Security Maintenance	Module 12	Domain 6 & 7	
15.		**Final Presentation: Organizational Security Assessment**	-	Integrated	
16.		**Final Exam**	(Module 1-12)	All Domains	

*The schedule and content may be subject to change.

Midterm Group Presentation: Real-World Cybersecurity Case Analysis (25%)

Objective

The objective of this assignment is to develop undergrade students' ability to analyze real-world cybersecurity and information security incidents by applying the concepts, principles, and frameworks learned in class. Students will investigate a real cyberattack or information security incident, identify its causes and impacts, evaluate the security failures involved, and propose practical recommendations based on industry best practices.

Group Formation

- Each group will select case for assessment.
- Each case may only be selected by one group (Come first get first).
- Topic approval is required before Week 8.

Presentation Requirements

1. Case Overview (10%)
   - Organization background
   - Date of incident
   - Brief description of the cybersecurity incident
2. Incident Analysis (20%)
   - What happened?
   - How did the attack occur?
   - Timeline of the incident
3. Security Vulnerabilities (20%)
   - Vulnerabilities exploited
   - Human factors
   - Technical weaknesses
   - Organizational weaknesses
4. Impact Assessment (25%)
   - Confidentiality, Integrity, and Availability (CIA)
   - Financial losses
   - Operational disruption
   - Reputation damage
   - Privacy and legal implications
5. Recommendations (25%):
   - Information security policies
   - Security awareness and training
   - Risk management practices
   - Organizational security procedures
   - General technical or administrative safeguards

Suggested Topics

Undergrade students are encouraged to choose recent (within the last 5–10 years) cybersecurity incidents (Any other instructor-approved cybersecurity incident), such as:

- CrowdStrike Global IT Outage (2024)
- Change Healthcare Ransomware Attack (2024)
- Snowflake Customer Data Breaches (2024)
- MGM Resorts Ransomware Attack (2023)
- MOVEit Transfer Vulnerability (2023)

- Colonial Pipeline Ransomware Attack (2021)
- SolarWinds Supply Chain Attack (2020)
- Twitter Bitcoin Scam (2020)
- Marriott Data Breach
- Equifax Data Breach
- Target Data Breach
- WannaCry Ransomware
- NotPetya Malware
- Stuxnet

Note

- Undergraduate students are expected to go beyond simply describing the incident. A strong presentation should explain why the incident occurred, identify the underlying security weaknesses, relate the case to the information security concepts discussed in class, and propose practical recommendations supported by appropriate cybersecurity principles or best practices.

Final Group Presentation: Organizational Security Assessment (30%)

Objective

Undergrade students will apply information security concepts, frameworks, and technologies to assess the security posture of a real or hypothetical organization and propose practical recommendations.

Group Formation

- Each group will select one organization for assessment.
- Each organization may only be selected by one group (Come first get first).
- Topic approval is required before Week 14.

Presentation Requirements

1. Organization Overview (15%)
   - Organization background
   - Business operations
   - Critical information assets
2. Threat and Risk Analysis (25%): Identify the organization's major security threats and evaluate the associated risks. Include:
   - Major threats and vulnerabilities
   - Potential impact on Confidentiality, Integrity, and Availability (CIA)
   - Risk prioritization (e.g., simple risk matrix)
3. Security Controls (30%): Evaluate existing or proposed security controls. Discuss appropriate controls such as:
   - Administrative controls
   - Technical controls
   - Physical controls

   Undergrade students are <u>not</u> expected to discuss every possible technology (e.g., IDS, MFA, CCTV). Instead, they should recommend the most appropriate controls for their chosen organization.
4. Security Improvement Recommendations (30%): Recommend practical strategies to improve the organization's security posture.
   - Address the identified risks
   - Be realistic and feasible
   - Include both technical and managerial perspectives

Suggested Organizations

Undergrade students may choose organizations from various sectors, including:

- Hospital
- University
- Bank

- E-commerce company
- Government agency
- Manufacturing company
- Small or medium-sized enterprise (SME)
- Logistics company
- Technology company
- Non-profit organization

Notes

- Undergrade students are encouraged to apply concepts covered throughout the course, including security governance, risk management, access control, cryptography, network security, incident response, and security maintenance.
- Groups should support their analysis with relevant standards, frameworks, and best practices (e.g., ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls, or the ISC2 CISSP CBK) where appropriate.
- The focus of the project should be on critical analysis and practical recommendations rather than simply describing technologies or listing security controls.