QUẢN LÝ VÀ ĐÁNH GIÁ AN TOÀN THÔNG TIN
(INFORMATION SECURITY MANAGEMENT AND ASSESSMENT)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: Quản lý và đánh giá an toàn thông tin (Information Security Management and Assessment)

Course code: SEC1407_CLC

Course type: Compulsory

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with foundational and practical knowledge of information security management, including security standards, policies, and legal regulations. It covers security assessment, risk evaluation, auditing, secure system operations, business continuity management, and incident response strategies.

Skills:

On successful completion of this course a student will be able to:

- Apply security standards, policies, and legal regulations to design and manage information security programs that meet organizational and regulatory requirements.
- Implement and evaluate security assessment methodologies, risk management strategies, secure system operations, and incident response measures to ensure compliance and resilience.

Attitude:

Students are required to actively participate in coursework, maintain consistent attendance, and complete assignments/projects.

3. Abstracts

This course provides both theoretical foundations and practical insights into the development, implementation, and management of information security measures to meet the requirements of organizations and regulatory bodies. The curriculum covers widely recognized national and international security standards, along with relevant legal regulations to ensure compliance and effective application of security solutions.

Additionally, the course equips students with knowledge of security assessment and testing, including security testing methodologies, risk evaluation, test result analysis, and security auditing. Furthermore, students will explore principles and measures to ensure secure system operations, maintain business continuity, and effectively respond to information security incidents.

4. Teaching and learning methods

Lectures: 32h

Exercises: 5h
Projects: 8h
Labs: 0h
Individual reading: 0h

5. Prerequisites: Fundamentals of Information Security- SEC1401_CLC

6. Learning outcomes

After completing this course, the student is able to:
[CLO1]: Explain foundational and advanced knowledge of information security management and security assessment methodologies
[CLO2]: Apply security management strategies to develop information security programs, assess risks, and implement risk control measures
[CLO3]: Implement and evaluate business continuity strategies, disaster recovery plans, and compliance with information security policies and laws

7. Assignment criteria

Learning outcomes	**Assignment criteria**
[CLO1] Explain foundational and advanced knowledge of information security management and security assessment methodologies	Chapter 1- Chapter 7
[CLO2] Apply security management strategies to develop information security programs, assess risks, and implement risk control measures	Chapter 2, Chapter 3, Chapter 4, Chapter 5
[CLO3] Implement and evaluate business continuity strategies, disaster recovery plans, and compliance with information security policies and laws	Chapter 6, Chapter 7

8. Outlines

Chapter 1: Overview of information security management

1.1. Information security issues
1.2. Information security objectives
1.3. Information security framework
1.4. Information security management
1.5. Principles of information security management
1.6. Information security policies and regulations

Chapter 2: Security planning

2.1. Introduction
2.2. Strategic planning
2.3. Key tasks

2.4. Organizing information security management
2.5. Classification of information and information systems

Chapter 3: Information security management system

3.1. Security management
3.2. Risk management
3.3. Risk identification, analysis, and evaluation
3.4. Risk control strategies
3.5. Best practices in risk control

Chapter 4: Information security standards

4.1. Global information security standards
4.2. ISO/IEC security standards
4.3. NIST security standards
4.4. Vietnam's information security standards

Chapter 5: Security assessment and testing

5.1. Overview of security assessment and testing
5.2. Conduct security control testing
5.3. Analyze test output and generate report
5.4. Conduct or facilitate security audits

Chapter 6: Business continuity and incident recovery

6.1. Principles of business continuity and incident recovery
6.2. Developing a business continuity plan (BCP)
6.3. Disaster recovery strategies
6.4. Testing and updating continuity plans

Chapter 7: Information security policies and laws

7.1 Policy and legal requirements
7.2 Information security laws in Vietnam
7.3 International legal frameworks for information security

9. Required Textbooks

[1] Michael E. Whitman, Herbert J. Mattord, Management of Information Security, Course Technology, Cengage Learning, 2018.

10. Suggested Textbooks

[2] Phạm Hoàng Duy, Information Security Lecture Notes, Posts and Telecommunications Institute of Technology, 2018.

[3] Mike Chapple, James Michael Stewart, Darril Gibson, CISSP® Certified Information Systems Security Professional Study Guide, 2018, John Wiley & Sons, Inc., ISBN: 978-1-119-47593-4.

[4] Michael E. Whitman, Herbert J. Mattord, Roadmap to Information Security: For IT and Infosec Managers, Delmar Publishers Inc., 2011.

[5] National Assembly of Vietnam, Information Technology Law (67/2006/QH11), July 12, 2006.
[6] National Assembly of Vietnam, Cybersecurity Law (86/2015/QH13), November 19, 2015.
[7] National Assembly of Vietnam, Cybersecurity Law (24/2018/QH14), June 12, 2018.
[8] Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 7th edition, Course Technology, Cengage Learning, 2021.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1: Overview of information security management	4h lecture	1.1. Information security issues 1.2. Information security objectives 1.3. Information security framework 1.4. Information security management 1.5. Principles of information security management 1.6. Information security policies and regulations
Chapter 2: Security planning	5h lecture 1h exercise	2.1. Introduction 2.2. Strategic planning 2.3. Key tasks 2.4. Organizing information security management 2.5. Classification of information and information systems
Chapter 3: Information security management system	5h lecture 4h project	3.1. Security management 3.2. Risk management 3.3. Risk identification, analysis, and evaluation 3.4. Risk control strategies 3.5. Best practices in risk control
Chapter 4: Information security standards	4h lecture 1h exercise 2h project	4.1. Global information security standards 4.2. ISO/IEC security standards 4.3. NIST security standards 4.4. Vietnam's information security standards
Chapter 5: Security assessment and testing	5h lecture 1h exercise 2h project	5.1. Overview of security assessment and testing 5.2. Conduct security control testing 5.3. Analyze test output and generate report 5.4. Conduct or facilitate security audits
Chapter 6: Business continuity and incident recovery	5h lecture 1h exercise	6.1. Principles of business continuity and incident recovery 6.2. Developing a business continuity plan (BCP) 6.3. Disaster recovery strategies 6.4. Testing and updating continuity plans

Chapter 7: Information security policies and laws	4h lecture 1h exercise	7.1 Policy and legal requirements 7.2 Information security laws in Vietnam 7.3 International legal frameworks for information security

12. Grading Policy

Attendance:	10%
Mid-term exam/exercises:	10%
Course projects:	30%
Final examination:	50%