ISC2 CHAPTER | Vietnam

Chapter Meeting

Topic: Security & Risk Management

Date: 17th April 2026

ISC2 CHAPTER | Vietnam

Agenda

1. About us
2. Why to discuss Security & Risk Management?
3. Security & Risk Management in Vietnam regulations
4. Security & Risk Management in practices
5. Q&A and community updates

ISC2 CHAPTER Vietnam

About us

- Founded since 2021
- ISC2 Vietnam is a non-profit community member of ISC2 the internationally recognized cybersecurity standards, education, and certification authority.
- We aim to advance and promote the greater Vietnam ecosystem of Cyber and Information System Security Professionals.

ISC2 CHAPTER Vietnam

Our History

Change from ISC2 HCMC Chapter to ISC2 Vietnam Chapter — **April 21st, 2025**

Vietnam Legal Entity Registration — **July, 2022**

Official Chapter Recognition — **June, 2022**

Creation of the HCMC Chapter — **October, 2021**

ISC2 CHAPTER Vietnam

Board Member

President

Mr. An Le

Vice President

Mr. Chuong Ngo

Vice President

Mr. Viet Nguyen

Vice President

Mr. Robert Leyba

Advisor

Mr. Phong Do

Community Manager

Ms. Nhi Vo

Advisor

Mr. Robert Tran

Advisor

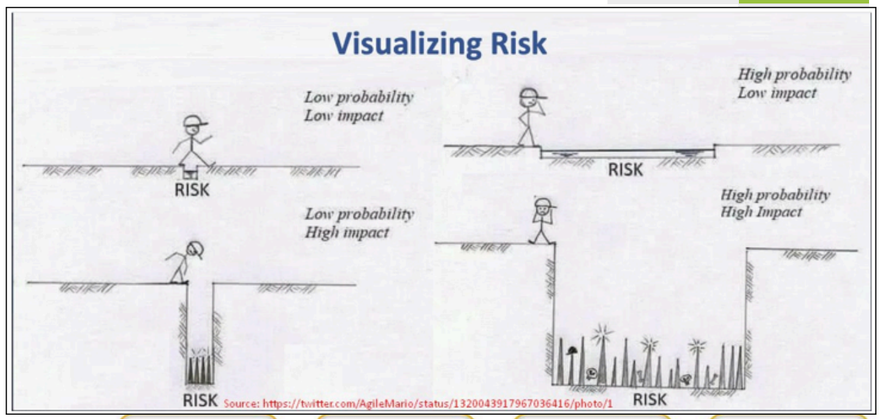
Mr. Charlie Chye

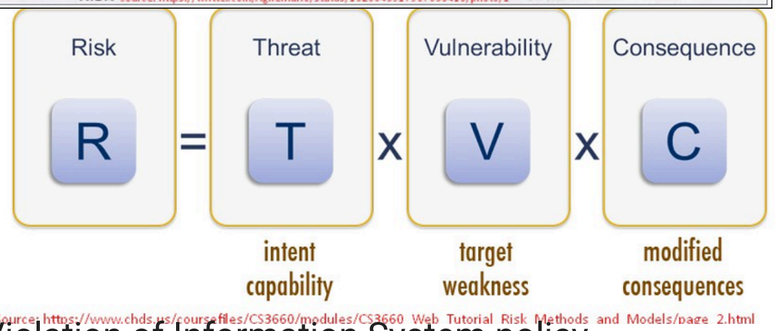
ISC2 CHAPTER Vietnam

Why to discuss Security & Risk Management?

1. **What is Risk?**

- ISO 31000 – “The effect of uncertainty upon an organisation’s ability to meet its objectives.”
- NIST SP 800-30 – “…a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.”





2. What are components of a risk?

- THREAT - The person/trigger that we are concerned about occurring (Threat/Threat actor)
- VULNERABILITY - The weakness or path through which the risk could occur
- CONSEQUENCE - A consequence is a damage that occurs because the threat took advantage of the vulnerability

Threats

- Human threats
- Environmental threats
- Technical and operational threats
- Cyber Threats

Vulnerabilities

- Hardware, software, or Network equipment and facilities.
- Business operations and service delivery.
- Physical environment.
- Personnel, management, and administrative procedures and controls of security controls.
- Violation of Information System policy
- Lack of Security Assessment
- Lack of Awareness session for employees
- Systems vulnerability
- Lack of configuration standards
- Lack of top management support

Source: https://www.experts-exchange.com/articles/35333/RISK-ASSESSMENT-METHODOLOGY.html

Why to discuss Security & Risk Management?

The threat landscape is continuously evolving, driven by emerging technologies such as AI and shifting geopolitical dynamics - both of which significantly influence cybersecurity risks, attack sophistication, and regulatory requirements.

Without risk management, security becomes a cost center driven by fear and tools - rather than a strategic function focused on protecting what truly matters to the business.

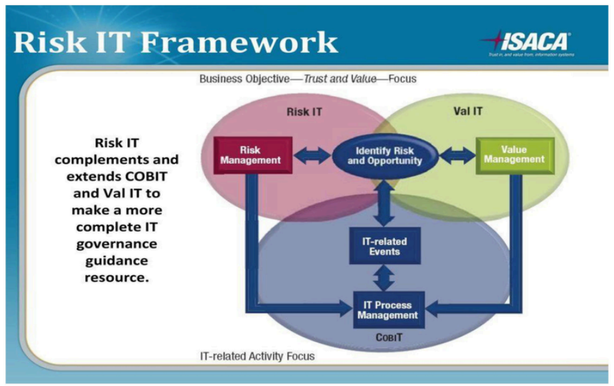
ISC2 CHAPTER Vietnam

Security & Risk Management in frameworks and standards

Frameworks and Standards provides the guildance for organization in implementing security & risk management. There is no universal framework - organizations must tailor their approach based on business objective, their maturity, industry demands, and risk appetite.

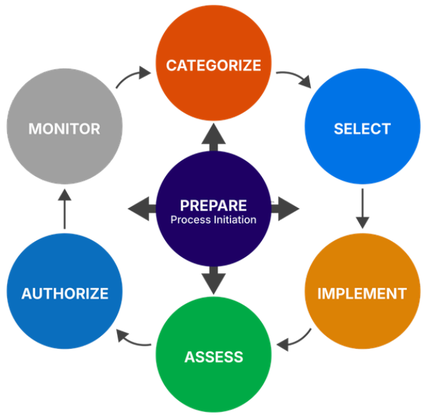
Popular Framework & Standards

ISACA Risk IT Framework



ISO 27001 & ISO 27005

NIST - 800-37



PCI DSS

ISC2 CHAPTER | Vietnam

Security & Risk Management in Vietnam regulations

Legal Document	Effective date	Article
Data Law No 60/2024/QH15	01/07/2025	5,15,22,25,27.
Cybersecurity Law No.116/2025/QH15	01/07/2026	All Articles
Law on Artificial Intelligence No 134/2025/QH15	01/03/2026	9, 10,12,13,14,15
Law on Digital technology Industry No 71/2025/QH15	01/07/2025	10, 25, 34, 41, 43, 45
Personal Data protection Law No 91/2025/QH15	01/01/2026	3, 12, 5,18, 19, 20,30,21,22, 25, 26, 27, 29, 30 31

All laws related to information technology has components of security & risk management. These requirements are mandatory for all IT system and data featured system.

ISC2 CHAPTER Vietnam

Security & Risk Management in practice

From Reality → Lessons Learned → Future Challenges

- Why security fails despite investments?
- What actually reduces risk?
- How Cloud & AI change the game?

ISC2 CHAPTER Vietnam

Security & Risk Management in practice

Reality: Security Still Fails — Even in Mature Organizations

- Tools are deployed
- Frameworks are adopted
- Policies are defined

Insight & Takeaway: The problem is not capability
→ It is **lack of clarity in risk & execution discipline**

Security & Risk Management in practice

Issue #1: Invisible Risk

The Problem

- You don’t know what truly matters
- Critical assets are not clearly defined

The Reality

- Full visibility is an illusion
- Asset inventory is always incomplete

What Works

- Define and protect **Crown Jewels first**
- Prioritize:
  - Critical systems
  - Sensitive data

Insight & Takeaway: You don’t manage all risks
→ You manage the **risks that can break the business**

ISC2 CHAPTER Vietnam

Security & Risk Management in practice

Issue #2: Unknown Risk

The Problem

- Threats evolve faster than controls
- Unknown attack paths remain unaddressed

The Reality

- Risk assessment is often outdated
- Organizations react, not anticipate

What Works

- Treat incidents as intelligence
- Build feedback loops:
  - Detect → Learn → Adapt

Insight & Takeaway: Risk management is not periodic
→ It is a **continuous learning system**

Security & Risk Management in practice

Issue #3: Compliance ≠ Security

The Problem

- Passing audits but still getting breached

The Reality

- Compliance creates a false sense of security
- Controls exist without real effectiveness

What Works

- Tie every control to a **real risk scenario**
- Focus on fundamentals

Insight & Takeaway: Compliance is necessary
→ But only valuable if it **reduces real-world risk**

ISC2 CHAPTER Vietnam

Security & Risk Management in practice

Issue #4: Execution Gap

The Problem

- Policies exist, but are not enforced
- Controls are implemented, but not effective

The Reality

- Security fails in day-to-day operations
- Ownership is unclear

What Works

- Automate wherever possible
- Assign clear accountability
- Continuously verify control effectiveness

Insight & Takeaway: Strategy doesn’t fail
→ Execution does

Security & Risk Management in practice

Future Challenge: Cloud & AI - A Fundamental Shift

What Changed

- Assets → Dynamic & ephemeral
- Risk → Rapidly evolving
- Control → Distributed

New Reality

- Identity is the new perimeter
- Data is the new attack surface

Insight & Takeaway: Traditional risk models break in modern environments
→ Risk management must become **adaptive & continuous**

Security & Risk Management in practice

Future Challenge: Emerging Risk Patterns

1. Loss of Visibility

- Multi-cloud, SaaS, shadow IT
  → Shift to **identity-centric security**

2. Data & AI Risk

- Uncontrolled data usage
- AI amplifies exposure
  → Require **data governance & control**

3. Speed vs Security

- DevOps & AI outpace security
  → Require:
- Automation & ZTNA
- Security embedded in pipelines

Insight & Takeaway: Security must move at the speed of the business
→ or it becomes irrelevant

ISC2 CHAPTER Vietnam

Security & Risk Management in practice - Takeaways

ISC2 CHAPTER Vietnam

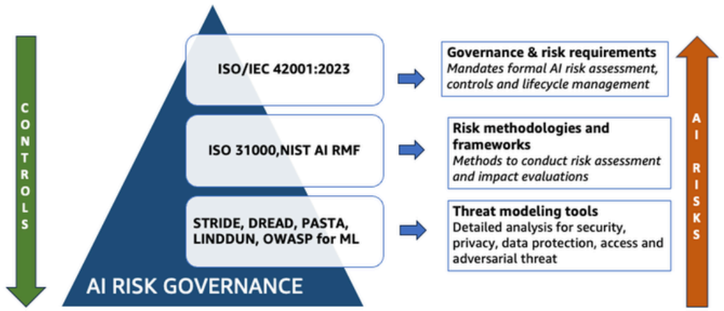
Q&A

ISC2 CHAPTER Vietnam

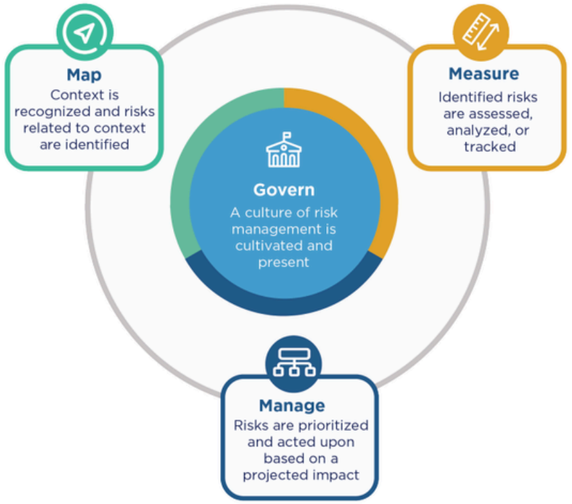
Security & Risk Management to adapt AI evolutions

AI Risk management operates from AI Risk Goverance to the detail frameworks and operations.

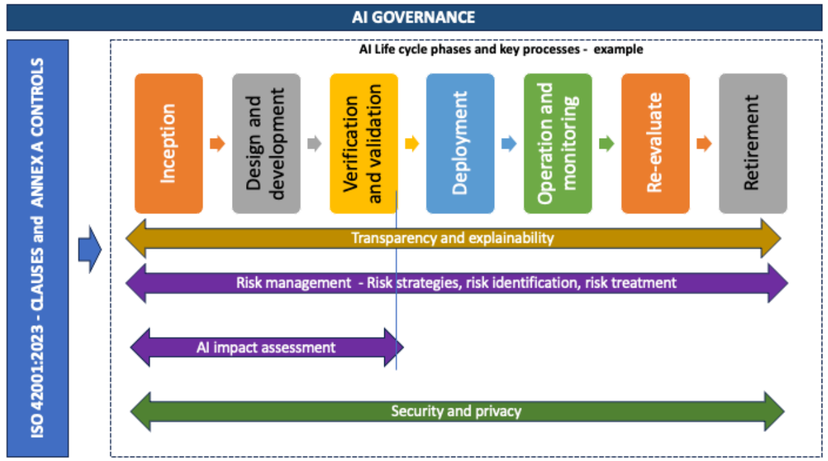
AI Risk Governance



NIST AI 100-1 AI



ISO/IEC 42001:2023



ISC2 CHAPTER Vietnam

ISC2 CHAPTER | Vietnam

Thank You

ISC2 CHAPTER | Vietnam