



# Risk Management for IT systems Training Course

1 – 5 November 2026  
Bangkok

## Risk Management for IT systems Training Course

**Ref:** 10\_85332 **Date:** 1 – 5 November 2026 **Location:** Bangkok **Fees:** 6000 Euro

### Overview

Every information system, from a payroll application to a cloud-hosted customer portal, carries its own set of threats, weaknesses and business consequences. This Risk Management for IT Systems course follows the system-level approach described in NIST guidance for information technology systems. Participants take one sample system through the complete cycle: describing its boundary, data and interfaces; listing threat sources; finding vulnerabilities through scans and configuration reviews; rating likelihood and impact; selecting technical, operational and management controls; weighing their cost against the risk reduced; and writing the risk assessment report and plan of action that system owners and authorising officials sign. This course is delivered by Agile Leaders Training Center.

### Who Should Attend

- Information system owners and application managers accountable for system risk
- Information security officers and analysts
- System and network administrators who maintain configurations and patches
- IT auditors and security assessors
- Software development and DevSecOps leads

### Departments and Industries

Suited to organisations that must assess and authorise individual information systems before and during operation.

- Information security, IT audit and software engineering
- IT infrastructure and applications
- Government IT, banking and payments
- Hospitals and health information, telecoms and cloud service providers
- Utilities with SCADA and IT systems

### Learning Objectives

By the end of this course, participants will be able to:

- Analyse an IT system's boundary, hardware, software, data flows and users.
- Build threat source and vulnerability lists using scan results, CVE data and configuration baselines.
- Evaluate likelihood and impact on confidentiality, integrity and availability and produce a risk-level matrix.
- Prioritise technical, operational and management controls and justify them with cost-benefit analysis.
- Apply security risk activities in each phase of the system development life cycle.

- Build a system risk assessment report and a plan of action and milestones for residual risk.

## **Course Agenda**

### **Day 1: IT System Risk in the Development Life Cycle**

- Why IT systems need their own risk assessment
- Roles: system owner, authorising official, security officer, assessor
- Risk activities in initiation, development, implementation, operation and disposal
- Security categorisation by the sensitivity of system data
- Introducing the case system and agreeing scope and roles for the assessment

### **Day 2: System Characterisation, Threats and Vulnerabilities**

- Documenting boundary, interfaces and data flows
- Human, natural and environmental threat sources
- Vulnerability scanning, penetration test findings and CVE lookups
- Security configuration baselines and hardening gaps
- Reviewing existing and planned controls to form threat and vulnerability pairs

### **Day 3: Likelihood, Impact and Risk Determination**

- Rating likelihood from threat capability and control strength
- Impact on confidentiality, integrity and availability
- Building and reading the risk-level matrix
- Qualitative versus quantitative approaches
- Documenting results for system owners in a ranked risk register

### **Day 4: Selecting and Justifying Controls**

- Technical controls: access control, encryption, logging, patching
- Operational and management controls
- Accept, avoid, limit or transfer: choosing an option per risk
- Cost-benefit analysis of proposed safeguards
- Calculating and accepting residual risk, with control recommendations for the case system

### **Day 5: Reporting, Authorisation and Continuous Monitoring**

- Writing the risk assessment report
- Plans of action and milestones for open findings
- Presenting to the authorising official, with final case report presentations
- Continuous monitoring and reassessment triggers
- Sample interview questions for assessors



## Practical Exercises

Working in small assessor teams on a web-based records application, participants complete these suggested activities.

- Suggested activity: fill in the system characterisation worksheet from architecture diagrams and an interview with the system owner.
- Suggested activity: build threat and vulnerability pairs from the catalogues and sample scan and configuration review outputs.
- Suggested activity: rate each pair on the likelihood, impact and risk-level matrix.
- Suggested activity: complete the control selection and cost-benefit worksheet and draft the report and plan of action.

## FAQs

### Does the course cover enterprise risk management?

No. It stays at the level of individual information systems rather than enterprise or operational risk in general.

### Do I need hands-on scanning experience?

No. Participants read and interpret sample scan and configuration review outputs; running scanning tools is not required.

### What documents will I produce?

A system description, a threat and vulnerability list, a risk matrix, control recommendations and a risk assessment report with a plan of action.

## Conclusion

Participants leave having produced the documents a security assessor actually delivers for an IT system: a system description, threat and vulnerability list, risk matrix, control recommendations and a report with a plan of action, ready to apply to risk management for IT systems in their own organisation.