
Information Security Risk Assessment and Treatment Training Course Using ISO/IEC 27005

22 – 26 March 2027
Milan





Information Security Risk Assessment and Treatment Training Course Using ISO/IEC 27005

Ref: 368_22995 **Date:** 22 – 26 March 2027 **Location:** Milan **Fees:** 5500 GBP

Programme Summary

Information security risk assessment and treatment using ISO/IEC 27005 is the subject of this five-day training course for information security managers, risk officers and CISOs at a managerial level, ending in a risk assessment and treatment pack for one organisation. Many risk registers cannot be traced to assets, scenarios or decisions. The programme moves from the standard and risk context, through diagnosis of assets, threats and existing controls, to analysis, evaluation and treatment design, then to application in one organisation. Mars Training Centre UK delivers this programme in information security risk assessment and treatment.

The Business Case

When information security risk is assessed on inconsistent scales, treatment spending follows habit rather than measured exposure. Leaders who fix the method, criteria and review rhythm can show why each risk was accepted, reduced, transferred or avoided, which matters when executives or auditors ask why a risk was tolerated and when security budgets compete with other priorities for limited funding.

- Treatment Spend: Aligns with exposure when risks share one scale.
- Audit Findings: Reduce as the register, plan and control selection trace to one another.
- Decision Speed: Improves when owners know the acceptance criteria and escalation thresholds in advance.

Principles and Evidence Base

- ISO/IEC 27005 guidance on managing information security risks: It supplies the process of context, identification, analysis, evaluation, treatment and monitoring that Sessions 1 to 4 follow.
- ISO/IEC 27001 requirements for information security management systems: They frame the risk assessment, treatment plan and control selection the participants prepare in Session 3.
- ISO 31000 principles and process for risk management: They shape the risk criteria, communication and review arrangements built in Sessions 1 and 4.

Intended Participants

- Security managers who own the information security risk process.
- Risk officers who consolidate security risks into enterprise reports.
- Security leaders who accept, fund or escalate treatment decisions.
- Management system leads and auditors who rely on risk records.

The programme serves banks, telecommunications, energy and public-sector technology teams.



Learning Outcomes

1. Participants will be able to evaluate an organisation's information security risk process against ISO/IEC 27005 and ISO/IEC 27001.
2. Participants will be able to diagnose gaps in asset, threat, vulnerability and control coverage.
3. Participants will be able to construct risk criteria, scales and acceptance thresholds.
4. Participants will be able to compare treatment options and design a risk treatment plan.
5. Participants will be able to prioritise residual risks for acceptance or escalation.
6. Participants will be able to justify a risk assessment and treatment pack to a security steering group.

Programme Structure

Day 1: Information Security Risk Principles, ISO/IEC 27005 and Risk Context

What does the standard ask of an information security risk process, and within what context does it run?

- ISO/IEC 27005 Process Overview
- ISO/IEC 27001 and ISO 31000 Links
- Scope and Boundary Statement
- Risk Ownership Matrix
- Risk Criteria and Acceptance Scale

Day 2: Diagnosing Assets, Threats, Vulnerabilities and Existing Controls

Where does the organisation hold value, and what threatens it today?

- Asset Inventory and Valuation Sheet
- Threat and Vulnerability Catalogue
- Existing Control Effectiveness Review
- Asset-Based Risk Identification
- Event-Based Scenario Identification

Day 3: Analysis, Evaluation and Risk Treatment Design

How are risks sized, ranked and treated, and which controls follow?

- Likelihood and Impact Rating Method
- Risk Evaluation Against Criteria
- Treatment Option Comparison
- Risk Treatment Plan Template
- Statement of Applicability Draft



Day 4: Communication, Monitoring and Review of Information Security Risk

How do decision makers see the risks, and how does the register stay current?

- Risk Register Structure
- Residual Risk Acceptance Record
- Key Risk Indicator Set
- Risk Communication Plan
- Reassessment Calendar

Day 5: Applying Information Security Risk Assessment and Treatment in One Organisation

Is the risk assessment and treatment pack ready for a steering group to adopt?

- Applying the Session 1 Criteria to the Chosen Organisation
- Testing the Session 2 Scenarios Against Existing Controls
- Checking the Session 3 Treatment Plan with Risk Owners
- Setting Monitoring Indicators from the Session 4 Set
- Completing the Risk Assessment and Treatment Pack

Methodology

The programme relies on structured exercises built on anonymised cases from banking, telecommunications and energy operators. Participants work in small teams as security manager, risk owner and internal auditor, and take one organisation from scope to a reviewed treatment plan.

- Suggested activity: Rating a set of scenarios on the agreed scale and defending each rating.
- Suggested activity: Choosing between reduce, retain, avoid and transfer for three risks.
- Suggested activity: Tracing one register entry to its controls in a draft statement of applicability.

Capstone Output

Each participant completes a risk assessment and treatment pack for one organisation. It holds a scope statement, risk criteria, a scenario list, an evaluated risk register, a treatment plan with owners, a draft statement of applicability and monitoring indicators. The pack briefs a steering group and prepares the next review.



Frequently Asked Questions

Is information security risk assessment and treatment suitable for managers who are not technical specialists?

Yes. Information security risk assessment and treatment is set at managerial level and assumes you own or rely on the risk process, not that you configure tools.

Which standards does information security risk assessment and treatment rest on in this training?

Information security risk assessment and treatment rests on ISO/IEC 27005, with ISO/IEC 27001 for the management system and ISO 31000 for risk management principles.

How is the pack from information security risk assessment and treatment used at work?

You use the information security risk assessment and treatment pack to brief a steering group, assign risk owners, fund treatment and schedule the next review.

How does information security risk assessment and treatment differ from a course on cybersecurity governance?

Information security risk assessment and treatment centres on a method for identifying, evaluating and treating risks, while cybersecurity governance centres on board oversight and accountability.