
IT Risk Registers, Control Design and Monitoring Indicators Training Course for Technology Leaders

8 – 12 February 2027
Milan





IT Risk Registers, Control Design and Monitoring Indicators Training Course for Technology Leaders

Ref: 305_20853 **Date:** 8 – 12 February 2027 **Location:** Milan **Fees:** 5500 GBP

Programme Summary

The IT risk register is the working tool at the centre of this five-day training course for technology, risk and audit leaders, and each participant leaves with an IT risk register and control plan for one technology environment. Technology failures now interrupt trading, expose data and draw regulator attention, yet many organisations hold risks in scattered lists that nobody scores the same way. The programme moves from identifying technology risks, through scoring and control design, to monitoring indicators and reporting, and then to a worked build. Mars Training Centre UK delivers this programme in IT risk registers and controls.

The Business Case

Technology risk is easy to describe and hard to compare. Systems outages, access failures, vendor dependence and change errors are logged by different teams in different formats, so executives cannot see which exposures matter most. An IT risk register that scores every entry on one scale, links it to named controls and tracks indicators over time gives leaders a common view and a basis for deciding where to spend.

- Risk Visibility: Improves as technology risks are recorded once, scored consistently and owned by named people.
- Control Effectiveness: Improves as each control is typed, tested and tied to the risk it addresses.
- Reporting Quality: Improves as indicators and thresholds replace anecdote in reports to senior committees.

Principles and Evidence Base

- ISACA IT Risk Framework: Its view of risk identification, assessment, response and monitoring structures the register work across Sessions 1 to 4.
- Likelihood and Impact Scoring: Rating each risk on likelihood and impact guides the scoring and ranking work in Session 2.
- Preventive, Detective and Corrective Controls: This classification guides the control design and gap analysis in Session 3.

Intended Participants

- Chief information officers and heads of technology who own the technology risk position.
- Risk and compliance managers who maintain registers and report to committees.
- Internal audit and assurance leads who test technology controls.
- Security and operations managers who run the controls day to day.



The programme serves banks, utilities, government bodies, telecommunications and other organisations that depend on complex systems.

Learning Outcomes

1. Participants will be able to identify technology risks across systems, data, vendors and change.
2. Participants will be able to score risks on likelihood and impact and rank them consistently.
3. Participants will be able to design preventive, detective and corrective controls for priority risks.
4. Participants will be able to evaluate control gaps against the risk appetite of the organisation.
5. Participants will be able to select monitoring indicators with thresholds and escalation rules.
6. Participants will be able to justify an IT risk register and control plan to a senior committee.

Programme Structure

Day 1: Identifying Technology Risks

Which technology risks does this organisation actually carry?

- Technology Asset and Service Inventory
- Threat and Vulnerability Identification
- Risk Statement Writing Standards
- Risk Ownership and Roles
- IT Risk Register Structure and Fields

Day 2: Scoring and Ranking Risks

How are technology risks scored so they can be compared?

- Likelihood Scale Definition
- Impact Scale Definition
- Inherent and Residual Risk Scoring
- Risk Heat Map Construction
- Risk Appetite and Tolerance Thresholds

Day 3: Designing and Testing Controls

Which controls reduce each priority risk, and do they work?

- Preventive Control Design
- Detective Control Design
- Corrective Control Design
- Control Gap Analysis
- Control Testing and Evidence Review



Day 4: Monitoring Indicators and Reporting

How do leaders know a technology risk is rising or falling?

- Key Risk Indicator Selection
- Threshold and Trigger Setting
- Incident and Near-Miss Trend Review
- Escalation Routes and Timelines
- Committee Reporting Format

Day 5: Applying the IT Risk Register to One Environment

Is the IT risk register and control plan ready for the senior committee?

- Populating the Register Using Session 1 Methods
- Scoring Entries with Session 2 Scales
- Mapping Controls from Session 3 to Each Risk
- Attaching Session 4 Indicators and Thresholds
- Completing the IT Risk Register and Control Plan

Methodology

The programme is built around structured exercises and case analysis. Participants work with anonymised incident summaries, system descriptions and control lists, build register entries in small teams, score them against agreed scales and defend their ranking to a simulated risk committee. Spreadsheet use is helpful, though no technical configuration skills are required.

- Suggested activity: Writing risk statements from three incident summaries.
- Suggested activity: Scoring and ranking a set of twelve technology risks.
- Suggested activity: Matching preventive, detective and corrective controls to a high-priority risk.

Capstone Output

Each participant completes an IT risk register and control plan for one technology environment. It contains scored risk entries, mapped controls, identified gaps, monitoring indicators with thresholds and a short note for the senior committee. It is used to brief the committee, to direct control investment and to set the next review cycle.

Frequently Asked Questions

Is IT risk register training suitable for leaders without a technical background?

Yes. IT risk register training is set at managerial level and assumes experience of oversight or reporting on technology, not hands-on engineering.



Which approaches does the IT risk register work rest on in this programme?

The IT risk register work rests on the ISACA IT Risk Framework, likelihood and impact scoring, and the classification of controls as preventive, detective or corrective.

How is the IT risk register used at work?

You use the IT risk register to rank technology exposures, direct control spending, brief senior committees and prepare for audit.

How does an IT risk register differ from a cybersecurity programme?

An IT risk register records and ranks all technology risks and the controls against them, while a cybersecurity programme concentrates on defending systems against attack.