



SOCI Act CIRMP Risk-Based Audit Training Course

25 – 29 January 2027
Milan

SOCI Act CIRMP Risk-Based Audit Training Course

Ref: 1274_194160 **Date:** 25 – 29 January 2027 **Location:** Milan **Fees:** 5700 Euro

Overview

SOCI Act CIRMP Risk-Based Audit Training Course is a one-week course for risk managers, internal auditors, governance professionals, control owners, and compliance leaders who need a CIRMP Assurance File. Participants scope applicable obligations, map material risks to controls, plan risk-based engagements, test design and operating effectiveness, evaluate evidence, and track remediation. The course connects SOCI Act compliance, CIRMP audit criteria, and critical infrastructure assurance. Agile Leaders Training Center presents CIRMP risk-based auditing as an evidence-led assurance practice.

Who Should Attend

- Functions responsible for critical infrastructure risk and governance
- Teams responsible for internal audit planning and engagement delivery
- Functions responsible for CIRMP ownership and control operation
- Teams responsible for compliance evidence and annual reporting
- Functions responsible for remediation monitoring and governing-body assurance

The course assumes participants already perform risk, control, compliance, or assurance work and leaves out introductory auditing, legal advice, and technical penetration testing.

Departments and Industries

The course supports departments and industries that operate or assure critical infrastructure assets subject to SOCI Act obligations.

- Internal audit, risk, compliance, and governance functions
- Operations, asset management, security, and technology functions
- Energy, utilities, transport, and communications organizations
- Financial services, data processing, and healthcare organizations
- Food, logistics, education, and research organizations

Learning Objectives

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



- Analyze SOCI Act applicability, asset scope, and CIRMP obligations
- Build audit criteria from all-hazards risk and governance requirements
- Apply risk-based planning to CIRMP assurance engagements
- Evaluate control design, operating effectiveness, and audit evidence
- Prioritize findings, causal factors, and remediation actions
- Use reporting and follow-up tools for governing-body assurance

Course Agenda

Day 1: Applicability and Audit Criteria

- SOCI Act Applicability and Obligation Map
- Critical Infrastructure Asset Scope Decision Tree
- Responsible Entity and Governance Responsibility Matrix
- Baseline, Enhanced, and Telecommunications CIRMP Scope Matrix
- CIRMP Audit Criteria and Evidence Matrix

Day 2: Risk and Control Traceability

- All-Hazards Risk Domain Taxonomy
- Material Risk and Relevant Impact Assessment Sheet
- Asset-Hazard-Control Traceability Register
- Interdependency and Operational Context Map
- CIRMP Currency and Review Control Checklist

Day 3: Engagement Planning and Evidence

- Global Internal Audit Standards Engagement Planning Framework
- CIRMP Risk-Based Audit Universe and Priority Matrix
- Engagement Objective, Scope, and Criteria Memo
- Audit Evidence Request and Sampling Plan
- Protected Information Handling Protocol

Day 4: Testing and Reporting

- Control Design Assessment Workpaper
- Operating Effectiveness Test Script
- Evidence Sufficiency and Reliability Evaluation Sheet
- Finding Significance and Root-Cause Analysis Record
- Remediation Ownership and Follow-Up Tracker

Day 5: CIRMP Audit Practice

- Exercise: SOCI Applicability and Asset Scope Assessment
- Exercise: Hazard-to-Control Traceability Review
- Exercise: Evidence and Control Test Evaluation
- Exercise: Annual Report and Governing-Body Assurance Briefing
- Capstone Exercise: CIRMP Assurance File

Practical Exercises

The course uses suggested activities that connect regulatory criteria, risk analysis, evidence testing, and assurance reporting.

- Suggested activity: determine applicable obligations for a transport asset and document the scoping rationale.
- Suggested activity: trace cyber, personnel, supply-chain, and physical hazards to controls for an energy asset.
- Suggested activity: test control evidence for a data-processing asset and evaluate finding significance.
- Suggested activity: prepare remediation priorities and a governing-body assurance briefing for a healthcare asset.

FAQs

Who should attend SOCI Act CIRMP risk-based audit training?

SOCI Act CIRMP risk-based audit training suits people who scope obligations, own risk and controls, perform internal audits, maintain compliance evidence, or report assurance. It assumes prior risk, control, compliance, or audit experience.

How does a CIRMP audit differ from general internal audit training?

A CIRMP audit applies risk-based engagement methods to SOCI Act applicability, all-hazards requirements, asset interdependencies, protected information, annual reporting, and control evidence, while general internal audit training covers engagement practices across many subjects.

What evidence supports a CIRMP audit conclusion?

CIRMP audit conclusions use relevant and reliable evidence such as approved governance records, risk assessments, control designs, implementation records, test results, incident records, review evidence, reporting records, and remediation status.



How are CIRMP audit findings prioritized?

CIRMP audit findings are prioritized by the significance of the underlying risk, the gap between criteria and condition, causal factors, potential effects, control dependence, and the urgency of corrective action.

How does CIRMP audit follow-up support annual reporting?

CIRMP audit follow-up tracks agreed actions, verifies closure evidence, reassesses residual exposure, and provides traceable assurance about program currency, variations, incidents, mitigation effectiveness, and governing-body oversight.

Conclusion

The course integrates SOCI Act applicability, CIRMP criteria, all-hazards risk analysis, engagement planning, evidence evaluation, control testing, findings, and follow-up. Participants take back a CIRMP Assurance File containing scope decisions, traceability records, workpapers, findings, and reporting materials. The file creates a repeatable path from regulatory obligation to tested control and monitored remediation.