CORE CONCEPT

Enterprise Risk Management (ERM): ISO 31000 and COSO ERM in Practice

Enterprise Risk Management (ERM): ISO 31000 and COSO ERM in Practice

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Many organisations keep risk registers that are updated once a year, rated inconsistently between departments and disconnected from strategy, budgets and board reporting. Risks that later cause losses were often recorded, but no one owned the response or saw how they combined. This Core Concept course equips managers to run enterprise risk management with ISO 31000 and COSO ERM, from building a common taxonomy to reporting principal risks to the board. Participants apply each method to case material from several sectors and leave with an ERM Framework and Implementation Roadmap.

Course Objectives

- Assess the maturity of an organisation's current risk practice and define a common risk language and taxonomy
- Apply the ISO 31000 process and the COSO ERM components to design a risk framework that fits the organisation
- Identify, analyse and evaluate enterprise risks using structured techniques selected from IEC 31010
- Build and maintain an enterprise risk register with named owners, controls, ratings and treatment plans
- Quantify and aggregate principal risks through scenario analysis and simulation, and report them to senior management and the board
- Produce an ERM Framework and Implementation Roadmap ready for executive approval

Target Audience

- Risk managers and ERM coordinators running the organisation-wide risk process
- Department and business unit managers who own operational and strategic risks
- Internal control, compliance and internal audit managers working alongside the risk function
- Finance and planning managers linking risk to budgets and performance targets
- Project and programme managers escalating project risks to the enterprise level
- Business continuity, health and safety and security managers coordinating specialist risk registers

Course Outline

Day 1: ERM Foundations and the Risk Context

- Risk Terminology and Definitions in ISO 31073:2022
- Enterprise Risk Taxonomy: Strategic, Financial, Operational and Compliance Risk
- IIA Three Lines Model: Roles in Enterprise Risk Management
- Emerging Risk Horizon Scanning with PESTLE and ISO/TS 31050:2023
- ERM Maturity Assessment Against the RIMS Risk Maturity Model

Day 2: Risk Management Frameworks and Standards

- ISO 31000:2018 Principles, Framework and Process
- COSO ERM 2017: Five Components and Twenty Principles
- ISO 31000 and COSO ERM Mapping Matrix
- IEC 31010:2019 Risk Assessment Technique Selection
- Risk Governance Structure: Risk Committee and Chief Risk Officer Mandates

Day 3: Assessing and Treating Enterprise Risk

- Risk Identification Workshops Using the Structured What-If Technique SWIFT
- Likelihood and Impact Scales and the 5x5 Risk Matrix
- Enterprise Risk Register Build: Owners, Controls and Ratings
- Bow-Tie Analysis of Causes, Consequences and Barriers
- Risk Treatment Options and Action Plan Templates

Day 4: Quantification, Culture and Risk Reporting

- Risk Interconnection Mapping and Heat Map Aggregation
- Scenario Analysis and Stress Testing of Principal Risks
- Monte Carlo Simulation for Risk Quantification
- Risk Culture Diagnosis with the IRM Risk Culture Aspects Model
- Board Risk Reporting and Principal Risk Dashboards

Day 5: Case Work and the ERM Implementation Roadmap

- Manufacturing Supply Disruption Case Study: Principal Risk Assessment
- Financial Services Case Study: Integrating Risk into Strategy and Budgeting
- Top-Ten Risk Profile Build for an Own Organisation
- ERM Framework and Implementation Roadmap Drafting
- Peer Review Panel and Roadmap Defence

Skills You Will Gain

- Risk Identification
- Risk Assessment and Rating
- Risk Register Management
- Risk Quantification
- Risk Treatment Planning
- Risk Culture Assessment
- Board Risk Reporting
- ERM Framework Design

Why Attend This Course

- Return to work with an ERM Framework and Implementation Roadmap for your own organisation, already tested by peers
- Replace inconsistent departmental ratings with one set of scales, one taxonomy and one register that management can compare
- Explain to executives which risks matter most, how they interact and what their treatment will cost
- Compare risk practice with managers from other sectors and countries who face similar reporting demands

Conclusion

Enterprise risk management only adds value when it shapes decisions rather than filling a register once a year. This course moves from a shared risk language and maturity baseline, through ISO 31000 and COSO ERM, to the assessment, quantification and reporting techniques that make principal risks visible to leadership. The final day turns that material into an ERM Framework and Implementation Roadmap that participants take back to their executives, giving them a structured and defensible basis for the next risk cycle they run.