CONCEPT

Compliance and Internal Controls: ISO 37301 and COSO Internal Control Framework

Compliance and Internal Controls: ISO 37301 and COSO Internal Control Framework

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

Introduction

Compliance failures rarely come from an unknown rule. They come from obligations no one mapped to a process, controls that exist on paper but are not operated, and testing that stops at design. Fines, remediation programmes and lost licences follow. This Core Concept course equips managers to build a working compliance and internal control programme with ISO 37301 and the COSO Internal Control framework, from the obligations register to board reporting. Participants apply each method to cases from several sectors and leave with a Compliance and Internal Control Programme Plan.

Course Objectives

- Compile a compliance obligations register and classify compliance risk by obligation, process and owner
- Apply ISO 37301 and the COSO Internal Control components and principles to design a compliance and control framework
- Build a risk and control matrix for a key process, including segregation of duties conflicts
- Plan and perform tests of control design and operating effectiveness, and grade the deficiencies found
- Investigate compliance breaches to root cause and report compliance status to senior management and the audit committee
- Produce a Compliance and Internal Control Programme Plan ready for management approval

Target Audience

- Compliance managers and officers running compliance programmes across functions
- Internal control managers and control owners responsible for control design and operation
- Finance, procurement and operations managers accountable for process controls
- Legal and company secretarial managers tracking regulatory and contractual obligations
- Risk and internal audit managers who assess and assure the control environment

Course Outline

Day 1: Compliance and Control Foundations

- Compliance Obligations Register: Mandatory Requirements and Voluntary Commitments
- Compliance Risk Taxonomy: Regulatory, Contractual, Conduct and Integrity Risk
- IIA Three Lines Model: Compliance, Control and Assurance Roles
- Compliance Function Charter: Mandate, Authority and Independence
- Control Environment Baseline Using a Compliance Maturity Self-Assessment

Day 2: Compliance and Internal Control Frameworks

- ISO 37301:2021 Compliance Management System Requirements and Amendment 1:2024
- COSO Internal Control—Integrated Framework 2013: Five Components and Seventeen Principles
- COSO Compliance Risk Management Guidance: Applying ERM to Compliance
- ISO 37001:2025 Anti-Bribery Management System Controls
- Preventive, Detective and Corrective Control Types and Entity-Level Controls

Day 3: Designing and Testing Controls

- Compliance Risk Assessment Matrix: Inherent Risk, Control Strength and Residual Risk
- Risk and Control Matrix RCM Build for a Key Process
- Segregation of Duties Conflict Matrix
- Process Narratives and Swimlane Flowcharts for Control Documentation
- Test of Design and Operating Effectiveness: Sampling and Evidence Standards

Day 4: Deficiencies, Breaches and Compliance Monitoring

- Control Deficiency Grading: Deficiency, Significant Deficiency and Material Weakness
- Root Cause Analysis of Compliance Breaches Using the 5 Whys
- Speak-Up Channels Aligned to ISO 37002:2021
- Continuous Controls Monitoring and Automated Control Testing
- Compliance Reporting to the Audit Committee: KPI and Issue Dashboard

Day 5: Case Work and the Programme Plan

- Procurement Process Case Study: Control Gap Analysis
- Healthcare Data Handling Case Study: Obligation Breach Response
- Risk and Control Matrix Completion for an Own Process
- Compliance and Internal Control Programme Plan Drafting
- Peer Review Panel and Programme Defence

Skills You Will Gain

- Obligations Mapping
- Compliance Risk Assessment
- Control Design
- Controls Testing
- Segregation of Duties Analysis
- Deficiency Evaluation
- Breach Root Cause Analysis
- Compliance Reporting

Why Attend This Course

- Return to work with a Compliance and Internal Control Programme Plan for your own function, already tested by peers
- Show auditors and management exactly which control covers which obligation, and what evidence proves it operates
- Grade control failures consistently and decide which ones must reach the audit committee
- Compare compliance practice with managers from other sectors and countries facing similar obligations

Conclusion

A compliance programme is only as strong as the controls that operate every day and the evidence that proves it. This course moves from mapping obligations and compliance risk, through ISO 37301 and the COSO Internal Control framework, to control design, testing, deficiency grading and breach investigation. The final day turns that material into a Compliance and Internal Control Programme Plan that participants take back to management, giving them a structured and auditable basis for meeting their obligations.