

Internal Compliance Investigations Training Course

9 – 13 November 2026
Vienna

AGILE LEADERS
Training Center

Internal Compliance Investigations Training Course

Ref: 1247_192121 **Date:** 9 – 13 November 2026 **Location:** Vienna **Fees:** 5700 Euro

Overview

Internal Compliance Investigations Training Course is a one-week advanced course for professionals who assess allegations and conduct internal inquiries, leaving with an Internal Compliance Investigation Plan, Evidence and Findings Pack. The course connects intake, independence, scope, evidence preservation, interviews, analysis, findings, reporting, root causes, remediation, and oversight. Agile Leaders Training Center frames internal compliance investigations through lawful, confidential, objective, and traceable casework.

Who Should Attend

- Teams responsible for receiving and assessing compliance allegations
- Teams responsible for internal investigations and case management
- Teams responsible for ethics, legal, employee relations, and disciplinary coordination
- Teams responsible for internal audit, risk, security, and fraud inquiries
- Teams responsible for speak-up systems, anti-retaliation, and case oversight
- Teams responsible for remediation, assurance, and governance reporting

The course assumes participants already handle sensitive cases or control reviews and leaves out criminal procedure, law-enforcement powers, and jurisdiction-specific legal advice.

Departments and Industries

The course supports departments and industries that investigate suspected misconduct or control failures.

- Compliance, ethics, legal, employee-relations, and human-resources departments
- Internal audit, risk, security, fraud, and assurance functions
- Financial services, insurance, professional services, and technology organizations
- Energy, construction, manufacturing, logistics, and healthcare operations
- Board, audit-committee, executive-office, and governance support teams

Learning Objectives

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

- Analyze allegations for credibility, severity, conflicts, and escalation
- Build an investigation mandate, scope, plan, and case chronology
- Apply evidence preservation and chain-of-custody controls
- Use structured interviews and credibility assessment methods
- Evaluate evidence against defined findings standards
- Prioritize root-cause, remediation, closure, and oversight actions

Course Agenda

Day 1: Intake, Independence, and Scope

- Allegation Intake and Preliminary Assessment Matrix
- Severity, Urgency, and Escalation Decision Tree
- Conflict Check and Investigation Independence Protocol
- Investigation Mandate, Scope, and Authority Document
- Confidentiality, Anti-Retaliation, and Need-to-Know Controls

Day 2: Planning and Evidence Control

- Investigation Plan, Issue List, and Case Chronology
- Evidence Source Map and Preservation Notice
- Document Collection and Chain-of-Custody Log
- Digital Evidence, Access, Privacy, and Legal Coordination Checklist
- Case Management File and Decision Audit Trail

Day 3: Interviews and Evidence Analysis

- Interview Strategy, Sequence, and Question Plan
- Witness, Subject, and Reporter Interview Protocol
- Interview Note, Confirmation, and Evidence-Corroboration Method
- Credibility Assessment and Inconsistency Matrix
- Document, Data, Timeline, and Relationship Analysis

Day 4: Findings, Reporting, and Remediation

- Evidence Evaluation and Findings Standard
- Allegation-by-Allegation Findings Matrix
- Investigation Report Structure and Executive Summary
- Root Cause Analysis and Control Failure Map
- Corrective Action, Discipline Interface, and Remediation Tracker

Day 5: Investigation Case Practice

- Exercise: Allegation Triage and Investigation Mandate
- Exercise: Evidence Map, Preservation Plan, and Custody Log
- Exercise: Interview Plan and Credibility Assessment
- Exercise: Findings, Root Cause, and Remediation Challenge
- Capstone Exercise: Internal Compliance Investigation Plan, Evidence and Findings Pack

Practical Exercises

The course uses suggested activities that turn allegations into controlled and reviewable investigation decisions.

- Suggested activity: triage a speak-up report and document severity, conflicts, independence, scope, and escalation.
- Suggested activity: build an evidence map, preservation plan, chronology, and chain-of-custody record.
- Suggested activity: prepare and conduct a structured witness interview using open, probing, and confirmation questions.
- Suggested activity: write findings, identify root causes, and assign remediation owners and closure evidence.

FAQs

Who is the Internal Compliance Investigations Course for, and what does it assume?

The course suits compliance, ethics, legal, audit, employee-relations, risk, security, and governance professionals. It assumes experience handling sensitive matters and does not provide jurisdiction-specific legal advice.

How does an internal compliance investigation differ from an internal audit?

An internal compliance investigation examines defined allegations and evidence to reach case findings, while an internal audit evaluates controls, processes, or assurance objectives across a broader planned scope.

How should evidence be managed in an internal compliance investigation?

Evidence should be identified, preserved, collected, logged, secured, analyzed, and disclosed on a controlled need-to-know basis with a traceable record of source, handling, decisions, and access.

How are internal compliance investigation findings supported?

Findings are supported by a defined proof standard, corroborated documents, data, interviews, timelines, credibility analysis, alternative explanations, and a clear link between each allegation and the evidence considered.

Conclusion

The course links allegation assessment, evidence, interviews, findings, and remediation in one investigation process. Participants take back an Internal Compliance Investigation Plan, Evidence and Findings Pack that makes authority, scope, decisions, evidence, findings, and actions traceable. The work product supports consistent case handling, defensible reporting, governance oversight, and control improvement.