JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Advanced AI Governance Training Course for Risk and Compliance Leaders

5 – 16 July 2027
Milan

# Advanced AI Governance Training Course for Risk and Compliance Leaders

**Ref:** 15_397 **Date:** 5 – 16 July 2027 **Location:** Milan **Fees:** 12400 GBP

AI Governance for risk and compliance leaders is a 2-week advanced training course for governance, risk, compliance, legal and AI programme heads, who leave with an AI governance operating model ready for board approval. AI systems now make or shape decisions on hiring, pricing, claims and public services, so boards must show who approved each system, on what evidence and under which limits. Jupiter Prime Training runs this course on AI governance for leaders carrying that accountability.

## Why AI Governance Matters Now

Three forces shape AI governance today: generative and agentic AI spreading through business units faster than policy can follow, boards and audit committees asking for assurance over systems they did not commission, and customers and supervisors expecting firms to justify automated outcomes. Organisations that govern AI well know every system they run, classify its risk and can stop it when it misbehaves; those that govern it badly discover shadow AI, unmanaged vendor models and incidents with no owner. Examples come from insurance claims handling and public sector service eligibility. The course rests on ISO/IEC 42001, the international standard for AI management systems, and the NIST AI Risk Management Framework AI RMF.

## Who Gains Most from AI Governance

- Enterprise risk heads who integrate AI into risk appetite, registers and reporting
- Compliance leads responsible for policy adherence and supervisory engagement on automated decisions
- General counsel and legal leads who allocate liability and review AI contracts and disclosures
- AI programme and transformation directors who need approval routes for new use cases
- Internal audit heads who plan assurance over AI systems and their controls

The greatest gain comes when the three lines of defence of one organisation, with its AI programme owner, attend together and agree a single approval path.

## AI Governance Capabilities

Participants move from scattered AI policies to a working system of decision rights, risk tiers, evidence and escalation that a board can rely on.

- Design AI policies and principles that translate into enforceable controls — the board and executive committee
- Apply an AI risk classification scheme and impact assessment method to proposed systems — use-case approval forums
- Build an AI system inventory with owners, tiers and lifecycle status — the chief risk officer
- Specify third-party AI due diligence and contract terms — procurement and legal
- Test AI controls through audit and assurance techniques mapped to ISO/IEC 42001 — the audit committee
- Communicate an AI governance operating model with roles, committees and incident response — directors and supervisors

## Key AI Governance Terms

- AI Management System AIMS — the policies, processes and controls an organisation uses to direct and oversee AI, as set out in ISO/IEC 42001.
- AI Risk Classification — sorting AI systems into tiers by potential harm so oversight intensity matches the stakes.
- AI System Inventory — an authoritative register of every AI system in use, with owner, purpose, risk tier and status.
- Algorithmic Impact Assessment — a structured review of an AI system's effects on people, rights and operations before and after deployment.
- Human Oversight — defined points where a person can review, override or halt an AI system's output.
- Shadow AI — AI tools adopted by staff or units without approval, inventory entry or risk review.

## AI Governance Day by Day

## Day 1: The AI Accountability Landscape

- AI Use Across the Enterprise — Mapping Decisions Delegated to Machines
- Generative and Agentic AI Risk Profile — New Failure Modes for Boards
- Stakeholder Expectations of AI Accountability — Customers, Staff and Supervisors
- Shadow AI Discovery Methods — Surfacing Unapproved Tools
- AI Governance Maturity Assessment — Baseline for Board Reporting

## Day 2: AI Policies and Principles

- AI Principles Statement — Fairness, Transparency, Safety and Accountability Commitments
- Acceptable Use Policy for Generative AI — Staff Permissions and Limits
- Policy-to-Control Translation — Turning Principles Into Testable Requirements
- Risk Appetite Statements for AI — Tolerances by Use-Case Type
- Policy Exception and Waiver Process — Documented Risk Acceptance

## Day 3: AI Management Systems With ISO/IEC 42001

- ISO/IEC 42001 Clause Structure — Context, Leadership, Planning and Operation
- AI Management System Scope Definition — Boundaries and Interfaces
- Annex Control Objectives — Selecting and Justifying Applicable Controls
- Statement of Applicability for AI — Evidence for Auditors
- Integration With Existing ISO Management Systems — Shared Processes

## Day 4: NIST AI RMF and Risk Classification

- NIST AI RMF Govern, Map, Measure and Manage Functions — Risk Lifecycle Fit
- Trustworthy AI Characteristics — Validity, Safety, Security, Privacy and Fairness Criteria
- AI Risk Tiering Matrix — Prohibited, High, Limited and Minimal Categories
- Risk Register Entries for AI Systems — Likelihood, Impact and Owners
- Key Risk Indicators for AI — Thresholds Triggering Escalation

## Day 5: Model Inventories and Impact Assessments

- AI System Inventory Design — Mandatory Fields and Update Triggers
- Use-Case Intake and Triage Workflow — Routing to the Right Review
- Algorithmic Impact Assessment Templates — Rights, Safety and Operational Effects
- Human Oversight Design Patterns — In-the-Loop, On-the-Loop and Out-of-Loop
- Post-Deployment Review Cycles — Reassessing Tier and Controls

## Day 6: Board Oversight and Accountability

- Board AI Oversight Charter — Committee Responsibilities and Reporting Lines
- Three Lines Model Applied to AI — First, Second and Third Line Duties
- Senior Accountable Owner Role for AI — Named Responsibility per System
- Board AI Dashboard Design — Metrics Directors Can Act On
- Director Questioning Frameworks — Challenging Management on AI Risk

## Day 7: Third-Party and Supply Chain AI Risk

- Vendor AI Due Diligence Questionnaires — Model, Data and Security Disclosures
- Contract Clauses for AI Services — Liability, Audit Rights and Model Changes
- Foundation Model Provider Dependencies — Concentration and Exit Planning
- Embedded AI in Purchased Software — Detecting Undisclosed Features
- Ongoing Vendor Monitoring — Performance and Incident Notification Terms

## Day 8: Audit and Assurance of AI

- AI Audit Universe and Risk-Based Audit Plan — Coverage Priorities
- Control Testing Procedures for AI — Design and Operating Effectiveness
- Algorithmic Audit Techniques — Bias, Robustness and Explainability Tests
- Assurance Reporting to the Audit Committee — Findings and Ratings
- Readiness for External Certification Audits — Evidence Packs

## Day 9: AI Incident Response and Continuous Oversight

- AI Incident Taxonomy — Harm, Malfunction, Misuse and Security Events
- Incident Response Playbook for AI — Detection, Containment and Kill Switches
- Root Cause Review for AI Failures — Data, Model or Process Origin
- Disclosure and Communication Decisions — Affected Parties and Supervisors
- Lessons-Learned Loop Into Policy — Updating Controls After Incidents

## Day 10: Practising the AI Governance Operating Model

- Governance Structure and Committee Design — Applying the Three Lines Model
- Approval Pathway by Risk Tier — Linking Intake, Assessment and Sign-Off
- Control Library and Assurance Plan — Mapping to ISO/IEC 42001 and NIST AI RMF
- Board Reporting and Incident Escalation Routes — Oversight Rhythm
- AI Governance Operating Model — Presentation for Board Approval

## Applying AI Governance After the Course

- Launch a shadow AI discovery exercise across business units and enter every system found into a tiered AI inventory with a named owner
- Run an algorithmic impact assessment on one high-tier AI system and present the findings and required controls to the risk committee

## AI Governance Questions FAQ

### What is AI governance and why does it matter now?

AI governance is the set of decision rights, policies, controls and oversight that keep an organisation's AI systems safe, lawful and aligned with its strategy. It matters now because AI spreads faster than policy, and boards must evidence control over it.

### Which roles gain most from AI governance training for risk and compliance leaders?

Enterprise risk, compliance, legal, internal audit and AI programme leaders gain most. They set policy, classify risk, approve systems and give assurance, so they need a shared method grounded in ISO/IEC 42001 and the NIST AI RMF.

### How does advanced AI governance training differ from an AI data governance course?

It governs AI systems as a whole rather than the datasets beneath them. You work on board oversight, risk tiering, approval pathways, vendor risk, audit and incident response, at a depth suited to leaders who already run risk or compliance functions.

## What do you bring back from AI governance training?

You bring back an AI governance operating model. It defines committees and roles, approval pathways by risk tier, a control library mapped to recognised frameworks, board reporting and incident escalation routes ready for board approval.

## AI Governance: The Way Forward

The AI governance operating model first informs which committee approves the next high-tier AI system and on what evidence. Boards, risk committees and AI programme owners use it to align approvals, assurance and reporting. After the first full approval cycle, revisit the risk tiering and incident data, since live systems often reveal harms the initial classification underweighted.