



# **AI and Machine Learning Policy and Oversight Training Course**

30 May – 3 June 2027  
Langkawi

## AI and Machine Learning Policy and Oversight Training Course

**Ref:** 194\_117671 **Date:** 30 May – 3 June 2027 **Location:** Langkawi **Fees:** 6000 Euro

### Overview

AI and Machine Learning Policy and Oversight Training Course is a five-day advanced course for policy owners, governance and risk leaders, compliance managers, model-risk personnel, auditors, legal advisers, and executives, who leave with a Policy and Oversight Operating Framework. Participants define AI policy scope, set machine learning risk tiers, build an AI system inventory, assign accountable ownership, establish human oversight controls, and organize assurance evidence and committee reporting. Agile Leaders Training Center delivers training in organizational AI policy oversight.

### Who Should Attend

- Policy personnel responsible for organization-wide AI principles, rules, and exceptions
- Governance and risk personnel responsible for risk classification, ownership, and approval controls
- Compliance and legal personnel responsible for obligations, evidence, and policy interpretation
- Model-risk and data personnel responsible for inventories, validation interfaces, and monitoring
- Internal audit and executive personnel responsible for assurance, challenge, and committee reporting

The course assumes participants can evaluate policies, risks, controls, and accountability at work, and it leaves out model development, coding, prompt engineering, and vendor-platform configuration.

### Departments and Industries

The course supports governance and oversight functions across financial services, healthcare administration, manufacturing, energy, technology services, and public services.

- Governance, enterprise risk, and compliance
- Legal, ethics, and policy management
- Internal audit and independent assurance
- Data, analytics, and model-risk management
- Technology, procurement, and third-party oversight

### Learning Objectives

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



- Analyze AI policy scope and lifecycle responsibilities
- Build use-case and model inventory requirements
- Apply risk tiers and approval gates
- Evaluate data, model, and third-party controls
- Design human oversight, monitoring, and incident paths
- Use assurance evidence for committee reporting

## **Course Agenda**

### **Day 1: Policy Scope and Governance Context**

- AI Policy Scope and Applicability Canvas
- AI System Lifecycle Responsibility Map
- NIST AI RMF Govern-Map-Measure-Manage Crosswalk
- ISO/IEC 42001:2023 Management-System Alignment Grid
- Policy Principles and Prohibited-Use Register

### **Day 2: Inventories, Risk Tiers, and Ownership**

- AI Use-Case and Model Inventory Schema
- Risk-Tier Classification Decision Tree
- Accountable Owner and Control-Function Matrix
- Approval Gate and Evidence Checklist
- Exception Request and Expiry Register

### **Day 3: Controls and Human Oversight**

- Data Provenance and Quality Control Map
- Model Limitation and Performance-Control Matrix
- Third-Party AI Due-Diligence Checklist
- Human Oversight and Decision-Rights Framework
- Transparency and Documentation Requirement Table

### **Day 4: Monitoring, Incidents, and Assurance**

- AI Performance and Risk Indicator Catalogue
- Control Monitoring and Evidence Calendar
- AI Incident Classification and Escalation Flow
- Policy Breach and Remediation Log
- Assurance Evidence and Committee Reporting Pack



## **Day 5: Policy Oversight Practice and Capstone**

- Suggested Exercise: Resolve an AI Policy Scope Question
- Suggested Exercise: Classify a Use Case by Risk Tier
- Suggested Exercise: Test an Approval Gate and Exception
- Suggested Exercise: Review an Incident and Assurance Pack
- Capstone Exercise: Policy and Oversight Operating Framework

## **Practical Exercises**

The course uses suggested activities that convert policy requirements into operational oversight artifacts.

- Suggested activity: distinguish covered use cases, excluded tools, policy owners, and lifecycle responsibilities
- Suggested activity: classify an AI use case and identify its approval, evidence, and human-review requirements
- Suggested activity: assess data, model, and third-party controls against an identified risk tier
- Suggested activity: assemble monitoring results, incident evidence, exceptions, and decisions for committee review

## **FAQs**

### **Who suits the AI and Machine Learning Policy and Oversight Training Course, and what does it assume?**

The course suits experienced governance, risk, compliance, legal, audit, data, and executive personnel who evaluate policies and controls without developing AI models.

### **How does AI policy and oversight training differ from machine learning development training?**

AI policy and oversight training focuses on scope, inventories, risk tiers, accountability, controls, monitoring, incidents, assurance, and reporting rather than algorithms, coding, data pipelines, or model implementation.

### **What should an AI and machine learning policy define?**

An AI and machine learning policy should define scope, principles, prohibited uses, inventory duties, risk tiers, owners, approval gates, human-review requirements, control expectations, monitoring, incident paths, exceptions, evidence, and review cadence.

## **How should organizations assign AI oversight responsibilities?**

Organizations should assign accountable business owners, policy custodians, control functions, technical evidence providers, independent challenge roles, approval authorities, incident responders, and committees with clear decision and escalation rights.

## **What evidence supports AI policy assurance?**

AI policy assurance uses current inventories, classifications, approvals, control tests, monitoring results, incidents, exceptions, remediation records, ownership decisions, and committee actions that can be traced to policy requirements.

## **Conclusion**

Participants take back a Policy and Oversight Operating Framework linking policy scope, inventories, risk tiers, ownership, controls, monitoring, incidents, and assurance evidence. It changes how governance teams convert policy statements into repeatable decisions and review records. The framework supports accountable approvals, visible exceptions, human oversight, independent challenge, and committee reporting.