AI Act Compliance Training Course: Risk Classes, Obligations and Readiness Planning

9 – 13 May 2027
Kuala Lumpur

AI Act Compliance Training Course: Risk Classes, Obligations and Readiness Planning

Ref: 904_41205 **Date:** 9 – 13 May 2027 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

AI Act compliance, covering risk classes, obligations and readiness planning under the EU AI Act, is the subject of this one-week training course for compliance, legal, risk and technology leaders at managerial level, ending in a readiness plan for one AI portfolio. Duties for organisations that build, buy or use AI depend on how each system is classified. The programme moves from the structure of the regulation to classification, provider and deployer duties, general-purpose models and readiness planning, using prepared system cases. Mars Training Centre UK delivers this programme on AI Act compliance to mixed-organisation cohorts.

The Business Case

Organisations that sell AI into the European market or use it there must know which systems fall under which duties before they are asked. Leaders who classify systems early, assign owners and gather evidence can plan the work in order and avoid costly rework on systems already in service.

- Regulatory Exposure: Falls when every system is classified and its duties are assigned to a named owner.
- Remediation Effort: Reduces when documentation and oversight gaps are found before a system is deployed.
- Supplier Assurance: Improves when provider and deployer duties are written into purchasing terms.

Principles and Evidence Base

- EU AI Act risk-based classification: The four tiers of prohibited practices, high-risk systems, limited-risk systems with transparency duties and minimal risk, applied in Sessions 1 and 2 to sort an AI inventory.
- EU AI Act duties for providers and deployers of high-risk systems: Risk management, data governance, technical documentation, record keeping, human oversight, accuracy and robustness, and conformity assessment, applied in Sessions 3 and 4.
- EU AI Act duties for general-purpose AI models and its phased timeline: Applied in Sessions 4 and 5 to sequence the work.

Intended Participants

- Compliance leaders who own regulatory change plans for technology.
- Legal advisers who interpret duties for providers and deployers.
- Risk managers who maintain inventories and control evidence for AI systems.
- Technology and data leaders who build or buy AI systems.
- Procurement leads who set supplier terms for AI tools.

Typical settings include financial services, healthcare, human resources technology and public services.

Learning Outcomes

1. Participants will be able to classify AI systems into the risk tiers of the EU AI Act.
2. Participants will be able to evaluate whether an organisation acts as a provider or a deployer for each system.
3. Participants will be able to construct an evidence file covering documentation, record keeping and human oversight.
4. Participants will be able to diagnose gaps in data governance, accuracy and robustness controls.
5. Participants will be able to prioritise remediation by risk tier, system status and the phased timeline.
6. Participants will be able to justify a readiness plan to a board or compliance committee.

Programme Structure

Day 1: AI Act Compliance Foundations

How is the EU AI Act built, and whom does it reach?

- Regulation Structure Map
- Risk Tier Overview
- Provider and Deployer Role Test
- AI System Inventory Template
- Scope Decision Sheet

Day 2: Risk Classification of AI Systems

Which tier does each system fall into, and why?

- Prohibited Practice Screen
- High-Risk Classification Test
- Transparency Duty Check
- Minimal Risk Register
- Classification Rationale Note

Day 3: Duties for High-Risk Systems

What must providers and deployers show for a high-risk system?

- Risk Management Record
- Data Governance Review
- Technical Documentation Outline
- Human Oversight Design
- Conformity Assessment Plan

Day 4: General-Purpose Models and Supplier Terms

How do model duties and supplier terms change the plan?

- General-Purpose Model Duty Map
- Accuracy and Robustness Evidence Review
- Record Keeping Specification
- Supplier Duty Clause List
- Phased Timeline Planner

Day 5: Readiness Plan for One AI Portfolio

Do the findings join into a plan a board can approve?

- Applying the Session 1 Inventory Template
- Testing the Session 2 Classification Rationale
- Checking the Session 3 Documentation Outline
- Reviewing the Session 4 Timeline Planner
- Completing the Readiness Plan

Methodology

The programme is a case analysis built on prepared descriptions of AI systems from a bank, a hospital group and a recruitment platform. Participants classify systems, assign provider and deployer roles, judge evidence files and plan remediation in small groups, then defend a readiness plan to peers acting as a compliance committee.

- Suggested activity: Classifying six systems and defending each tier in a short challenge round.
- Suggested activity: Reviewing a documentation file and listing the missing evidence.
- Suggested activity: Drafting supplier clauses for a high-risk tool.

Capstone Output

Each participant completes a readiness plan for one AI portfolio. It holds the system inventory, classification rationale, role assignments, an evidence gap list and a sequenced remediation timeline. At work it goes to the compliance committee for approval and becomes the reference for classifying each new AI system.

Frequently Asked Questions

Is AI Act compliance suitable for leaders who are not lawyers?

Yes. AI Act compliance is taught through prepared system cases and templates. You need responsibility for compliance, risk, technology or procurement decisions, but no earlier legal training or knowledge of the regulation.

Which framework does AI Act compliance rest on in this programme?

AI Act compliance here rests on the EU AI Act: its four risk tiers, its duties for providers and deployers of high-risk systems, and its duties for general-purpose AI models on a phased timeline.

How is the readiness plan from AI Act compliance used at work?

You take the readiness plan to your compliance committee, use its classification rationale to sort each new system, and keep its remediation timeline as the order of work.

How does AI Act compliance differ from a programme on data protection?

AI Act compliance concentrates on classifying AI systems and meeting duties that follow from their risk tier, while a programme on data protection concentrates on handling personal data lawfully.