

AI Audit Mastery: Governance, Risk & Ethics

22 – 26 February 2027
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

AI Audit Mastery: Governance, Risk & Ethics

Ref: 103600423_61841 **Date:** 22 – 26 February 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Automated decision-making and machine learning architectures introduce operational, ethical, and oversight demands that traditional IT controls cannot address alone. This AI audit training provides internal auditors, risk managers, and technology leaders with systematic methods to evaluate algorithms, establish oversight structures, and test automated workflows. Participants examine structured techniques for AI risk control strategies, model validation, algorithmic bias testing, and data privacy safeguards across the development lifecycle. Through practical audit programmes, risk matrices, and case analysis, practitioners learn how to assess automated systems against governance standards and produce defensible assurance reports. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Internal and external auditors seeking specialized procedures to assess machine learning and automated workflows.
- IT auditors and compliance professionals responsible for verifying supervisory controls and data governance.
- Risk management and governance leaders establishing oversight policies for automated technologies.
- Cybersecurity professionals evaluating automated threat surfaces, access boundaries, and model integrity.
- Data scientists and technical leads preparing model documentation for independent assurance reviews.
- Governance consultants advising enterprise clients on ethical controls and algorithmic risk protocols.

Departments and Industries

This programme supports assurance and oversight specialists across data-intensive sectors adopting machine learning platforms.

- Internal Audit and Assurance Departments in Financial Services and Banking
- Risk Management and Compliance Divisions in Healthcare and Pharmaceuticals
- Technology Governance and Security Teams in Telecommunications and Software
- Governance and Ethics Review Committees in Government and Public Administration
- Quality Assurance and Systems Control Units in Industrial Manufacturing
- Advisory and Independent Review Practices in Professional Services

Learning Objectives

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

- Conduct structured AI audits aligned with recognized governance frameworks and internal control principles.
- Identify and evaluate operational, legal, and ethical exposures across machine learning workflows.
- Evaluate AI model risk management practices and determine compliance with supervisory standards.
- Perform systematic assessments for algorithmic bias, fairness, transparency, and data privacy.
- Apply specialized AI risk assessment tools to verify data lineage, model drift, and system security.
- Trace machine learning lifecycles from data collection to active deployment to confirm supervisory controls.

Course Agenda

Day 1: AI Governance and Audit Frameworks

- Structural foundations of governance and accountability in automated systems
- Audit compliance parameters and internal control expectations for machine learning
- Overview of AI risk assessment tools and assurance methodologies
- Ethical dimensions and organizational values in automated decision review
- Auditing system lifecycles from model design to operational deployment
- Structured review of assurance frameworks and audit charter alignment

Day 2: Risk Management and Ethical Controls

- Organizational governance models, oversight committees, and operational roles
- Risk identification, impact scoring, and threat mitigation in intelligent systems
- Data privacy in auditing: data provenance, processing records, and consent verification
- Establishing control baselines to satisfy evolving regulatory obligations
- Evaluating algorithmic bias, demographic parity, and accountability measures
- Review session on embedding risk controls into operational business units

Day 3: Risk Assessment Tools and Model Auditing

- Deploying standardized assessment templates across complex data pipelines
- Verification techniques for technical security, access controls, and data integrity
- Audit procedures for validating machine learning model design and data inputs
- Practical case evaluation: conducting an assurance review on clinical automation
- Quantitative testing methods for detecting bias and evaluating fairness
- Review session on evidence collection standards and technical testing logs

Day 4: Model Governance and Decision Transparency

- Governance frameworks for model evaluation, validation, and change management
- Continuous monitoring mechanisms to detect model drift and performance anomalies
- Assurance roles in pre-deployment model sign-off and operational supervision
- Auditing explainability mechanisms and automated decision traceability
- Legal liability, supervisory expectations, and ethical risk containment
- Simulated walkthrough of internal control testing on predictive algorithms

Day 5: Audit Execution and Assurance Reporting

- Consolidated review of technical testing tools and control evaluation methods
- Practical integration of model audits into enterprise risk management frameworks
- Simulation exercise: preparing and conducting an automated workflow audit
- Assessing organizational control maturity, escalation paths, and supervisory boards
- Drafting the final assurance report: findings, risk ratings, and remediation plans
- Action planning session: operationalizing audit work programmes within the organization

Course Toolbox

- Standardized audit programmes and testing workpapers for automated systems
- Checklists for evaluating governance structures and ethical control measures
- Risk assessment matrix templates for data quality, model drift, and security
- Sample workbooks for testing algorithmic bias, fairness metrics, and explainability
- Reporting templates with findings classification matrices and remediation tracking sheets

Frequently Asked Questions

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should ideally have experience in IT auditing, risk management, compliance, or information security. Basic familiarity with technology infrastructure and core internal audit principles is recommended to fully engage with the technical assurance concepts.

How long is each day's session, and is there a total number of hours required for the entire course?

Each session lasts approximately 4 to 5 hours, incorporating interactive lectures, exercises, and discussions. The full course spans five consecutive days, delivering 20 to 25 hours of focused professional instruction.

Can AI auditing tools be used in real-time auditing?

Yes, specialized monitoring and testing tools can interface with operational data pipelines to observe model performance, flag unexpected drift, and track algorithmic decisions continuously alongside scheduled periodic audits.

How This Course Compares

This course focuses on practical internal audit execution, model governance structures, and ethical control testing. Unlike high-level compliance overviews or purely technical data science programmes, this curriculum bridges organizational oversight with concrete audit workpapers. Participants gain actionable testing methods to assess automated algorithms, verify data privacy, and deliver defensible audit reports that satisfy executive committees and supervisory bodies.