AI Risk Management & Compliance: Auditing Intelligent Systems Across the Lifecycle

5 – 9 July 2027
New York

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

AI Risk Management & Compliance: Auditing Intelligent Systems Across the Lifecycle

Ref: 51_86387 **Date:** 5 – 9 July 2027 **Location:** New York **Fees:** 12000 Euro

Overview

Organizations deploying automated technologies encounter significant challenges concerning model reliability, algorithmic bias, data lineage, and operational security. This five-day course establishes rigorous methodologies for AI risk management & compliance across every phase of system development and deployment. Participants evaluate computing infrastructure, inspect training data integrity, conduct model validation, and verify human-in-the-loop oversight mechanisms. The curriculum presents systematic audit workflows, technical risk indicators, and governance protocols to ensure automated decisions remain transparent, accountable, and operationally resilient. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Chief information security officers and enterprise risk managers evaluating automated decision systems.
- Internal and external auditors responsible for assessing algorithm governance and data pipelines.
- Compliance officers and legal specialists monitoring adherence to statutory transparency standards.
- System architects and machine learning engineers implementing technical control frameworks.
- Governance committee members overseeing the ethical deployment and operational safety of machine intelligence.

Departments and Industries

This programme supports technical, compliance, and governance professionals across sectors implementing automated decision workflows.

- Information Security and Risk Management in Banking and Financial Services
- Regulatory Compliance and Internal Audit in Healthcare and Life Sciences
- Data Science and Software Engineering in Telecommunications and Technology
- Safety and Systems Quality Assurance in Manufacturing and Autonomous Robotics
- Corporate Governance and Public Sector Technology Oversight Bodies

Learning Objectives

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

- Conduct structured technical reviews for auditing intelligent systems throughout their operational lifecycle.
- Establish operational controls aligned with international AI risk management frameworks.
- Perform algorithmic audits to detect bias, drift, and lack of explainability in machine learning outputs.
- Evaluate computing hardware, edge processing nodes, and sensor interfaces for security vulnerabilities.
- Inspect data pipelines, lineage tracking, and privacy-preserving transformations across distributed environments.
- Formulate audit findings into defensible governance reports featuring risk scoring and corrective action plans.

Course Agenda

Day 1: Foundations of AI Risk and Governance

- Core concepts in AI risk management frameworks and international governance benchmarks
- Accountability structures and operational responsibility in automated decision processes
- Auditor independence, evaluation standards, and evidence gathering protocols
- Defining trustworthy systems through transparency, explainability, and predictability metrics
- Scoping audit assessments using operational use cases and risk classification tiers
- Mapping statutory baseline requirements and organizational policy obligations

Day 2: Infrastructure and Data Governance Auditing

- Infrastructure evaluation for specialized computing units and distributed cloud environments
- Hardware security, sensor calibration risks, and data capture vulnerabilities at the edge
- Data quality, provenance verification, and governance of synthetic training datasets
- Privacy impact evaluations, data minimization, and retention controls
- Software bill of materials and AI supply chain third-party vendor assessments
- Cross-border data movement controls and distributed architecture assurance

Day 3: Model Validation and Explainable AI

- Algorithmic risk evaluation across supervised, unsupervised, and reinforcement architectures
- Model fine-tuning review, validation checkpoints, and performance drift metrics
- Overfitting detection, generalization assessment, and boundary condition stability checks
- Fairness audits, bias detection workflows, and disparity measurement techniques
- Explainable AI toolkits, interpretability evaluations, and feature attribution methods
- Assessing federated learning architectures and generative model behavior

Day 4: Security, Controls and Human Oversight

- AI cybersecurity reviews including intrusion detection, model poisoning, and evasion testing
- Interface evaluations covering automated recommendations and operator interaction controls
- Operational resilience, system redundancy, and physical security parameters
- Hierarchical and behavior-based automated control mechanism evaluations
- Governance models for human-in-the-loop, on-the-loop, and autonomous operational states
- Decommissioning workflows, fail-safe mechanisms, and system termination triggers

Day 5: Lifecycle Assurance and Audit Reporting

- Standardized checklist integration for hardware, pipeline, and algorithmic components
- Documentation review across training registries, code repositories, and operational logs
- Establishing internal policy frameworks and continuous lifecycle control gates
- Readiness reviews against established industry assurance benchmarks
- Structuring defensible audit reports, severity scoring matrices, and evidence files
- Formulating corrective mitigation roadmaps and stakeholder governance presentations

Practical Exercises

Participants complete applied audit simulations to evaluate technical evidence and draft control findings.

- Suggested activity: Conduct an algorithmic bias assessment on a sample classification model using parity metrics.
- Suggested activity: Perform a data pipeline audit verifying lineage, consent tracking, and sanitization records.
- Suggested activity: Design a human-in-the-loop escalation matrix for automated operational decision failures.
- Suggested activity: Draft an intelligent system audit finding report with severity ratings and corrective actions.

FAQs

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

There are no strict prerequisites; however, participants with backgrounds in risk management, auditing, compliance, AI development, cybersecurity, or legal governance will benefit most. Foundational knowledge of modern information technology systems and data privacy principles is recommended.

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

Each day's session is structured to last around 4 to 5 hours, with breaks and interactive activities included. The total course duration spans five days, providing approximately 20 to 25 hours of focused instruction.

What is the difference between auditing an AI system and evaluating compliance with AI regulations?

Auditing an AI system involves evaluating its operational performance, algorithmic integrity, transparency, and resilience across its complete operational lifecycle. Compliance checks focus strictly on whether specific baseline statutory mandates are satisfied. This programme equips professionals to evaluate overall system trustworthiness beyond basic regulatory checklists.

Conclusion

Organizations relying on automated technologies must substantiate system safety, accountability, and operational integrity. By mastering technical audit protocols, infrastructure reviews, and model validation techniques, participants gain the capability to protect operational workflows against unforeseen liabilities and maintain resilient enterprise oversight.