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

15 - 19 Sep 2025
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

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

Ref.: 51_37007 **Date:** 15 - 19 Sep 2025 **Location:** Kuala Lumpur **Fees:** 5200 **Euro**

Course Overview:

The course is a cutting-edge corporate training program designed to equip professionals with the knowledge and methods needed to proactively manage AI risk across every stage of the AI system lifecycle. This course presents a practical framework that transcends regulatory checklists to promote trustworthy, explainable, and resilient AI systems. Participants will learn how to assess AI resilience and robustness, perform evaluations throughout the AI audit lifecycle, apply privacy-preserving technologies, and understand the intricacies of AI accountability, liability, and governance standards. Through real-world case studies and structured methodologies, this course empowers auditors, compliance officers, and AI professionals to tackle risks related to bias, data provenance, federated learning, cloud auditing, and AI cybersecurity. Participants will leave with the confidence to lead AI risk assessments, develop ethical AI audit frameworks, and integrate AI risk governance into corporate strategy.

Target Audience:

- Chief Information Security Officers CISOs
- AI Compliance Officers
- Internal and External Auditors
- AI System Developers and Architects
- Risk Managers and Governance Professionals
- Legal and Compliance Specialists

Targeted Organisational Departments:

- Information Security and Risk Management
- Compliance and Internal Audit
- Data Science and AI Development Teams
- Legal Affairs and Corporate Governance
- Information Technology Infrastructure
- Research and Innovation

Targeted Industries:

- Financial Services
- Healthcare and Life Sciences
- Manufacturing and Robotics
- Government and Defence
- Telecommunications and Technology
- Energy and Smart Infrastructure

Course Offerings:

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

- Conduct end-to-end intelligent systems auditing across the AI lifecycle
- Implement AI risk mitigation strategies aligned with global governance standards
- Evaluate AI resilience, robustness, and explainability
- Apply AI accountability and liability principles in assessments
- Validate AI models and assess algorithmic fairness
- Identify and manage risks related to data quality, privacy, sensors, and control systems
- Assess AI supply chain vulnerabilities and federated learning implementations
- Conduct AI privacy impact assessments and documentation audits

Training Methodology:

This highly interactive training combines theory with practical application using real-world scenarios and emerging audit methodologies from the CSA guidance. Participants will engage in group exercises, simulations of AI risk evaluation, and audit checklists aligned with the Artificial Intelligence Risk Management Framework AI RMF. Case studies include risk reviews for federated learning, AI cybersecurity auditing, human-in-the-loop designs, and fog/cloud systems. Methods like AI audit templates, explainability toolkits, and bias detection frameworks will be demonstrated. Feedback sessions and peer-reviewed group work ensure critical thinking, while structured reflection builds problem-solving capacity for complex AI auditing challenges. The course leverages AI governance standards and sample audit questions from the CSA to enable a lifecycle-based approach to AI assurance.

Course Toolbox:

- AI Risk Assessment Templates
- AI Privacy Impact Assessment Frameworks
- Explainable AI XAI Toolkits
- AI Model Validation & Fine-Tuning Guidelines
- Checklists for AI Lifecycle Auditing based on CSA Appendices
- Case Studies in Federated Learning & Sensor Risks
- Cloud/Fog AI Audit Examples
- Human-in-the-Loop Oversight Protocols
- AI Regulatory Mapping Tools GDPR, EU AI Act, etc. Demo
- AI Governance Maturity Models

Course Agenda:

AGILE LEADERS
Training Center

Day 1: Foundations of AI Risk, Governance & Accountability

- **Topic 1:** Understanding AI Risk Management Frameworks and Global Standards
- **Topic 2:** Accountability, Responsibility, and Legal Liability in Intelligent Systems
- **Topic 3:** Auditing the Auditor: Competence, Ethics, and Independence
- **Topic 4:** Defining Trustworthy AI: Transparency, Explainability, and Predictability
- **Topic 5:** Use Cases as Risk Anchors: Contextualising Audit Scope and Metrics
- **Topic 6:** Overview of Applicable Laws, Regulations, and Compliance Requirements
- **Reflection & Review:** Beyond Compliance – Applying Governance in Real AI Scenarios

Day 2: Infrastructure, Data Governance & Sensor Risk

- **Topic 1:** Auditing Infrastructure for AI: Hardware, Connectivity, and Energy Efficiency
- **Topic 2:** Evaluating Data Processing Units CPU, GPU, TPU, Edge Computing
- **Topic 3:** Risks in Sensor Design, Calibration, and Data Capture Mechanisms
- **Topic 4:** Assessing Data Governance: Quality, Lineage, and Organic vs Synthetic Data
- **Topic 5:** Privacy Impact Assessment: Consent, Retention, and Cross-Border Compliance
- **Topic 6:** AI Supply Chain and Vendor Risk Assessment SAIBOM & Third-Party Audits
- **Reflection & Review:** Lifecycle Risk Mapping – Infrastructure to Data Flow Analysis

Day 3: Algorithms, Models & Explainable AI

- **Topic 1:** Algorithmic Risk: Auditing Supervised, Unsupervised & Reinforcement Learning
- **Topic 2:** Model Training, Fine-Tuning, and Validation Techniques LoRA, F1 Metrics
- **Topic 3:** Overfitting, Generalisation, and Performance Stability Audits
- **Topic 4:** Fairness, Bias Detection, and Ethical AI Auditing
- **Topic 5:** XAI: Explainability, Interpretability, and Trust in Model Decisions
- **Topic 6:** Auditing Advanced Learning: Federated, Few-shot, Zero-shot, and GANs
- **Reflection & Review:** Model Lifecycle Simulation – Audit Walkthrough of a Risky AI System

Day 4: Security, Interfaces, Controls & Human Oversight

- **Topic 1:** AI Cybersecurity Auditing – SIEM, IDS, Continuous Monitoring & Zero-Trust
- **Topic 2:** Interface Risk Audits: AR/VR, BCIs, Haptics, and UI Personalization Ethics
- **Topic 3:** Power Supply & Physical Security – Operational Resilience Audits
- **Topic 4:** Control Systems Auditing – Hierarchical, Behavior-Based, Hybrid Controls
- **Topic 5:** Human-in-the-Loop, On-the-Loop, and Out-of-the-Loop Governance Models
- **Topic 6:** Decommissioning and Fail-Safe Audits Kill Switch, Shutdown Protocols
- **Reflection & Review:** Intelligent Systems Threat Simulation & Defense Exercise

AGILE LEADERS
Training Center

Day 5: Documentation, Certification & Lifecycle Governance

- **Topic 1:** Review of CSA Appendices – Audit Checklists for AI Components
- **Topic 2:** Auditing Training Records, End-User Documentation & Dev Logs
- **Topic 3:** Developing Internal AI Governance Policies & Lifecycle Controls
- **Topic 4:** Preparing for Certification: CPD, ISO, CSA, and Industry Alignment
- **Topic 5:** AI Regulatory Readiness Assessments EU AI Act, GDPR, DORA, NIST RMF
- **Topic 6:** Final Audit Report Structuring: Scoring, Evidence, and Improvement Plans
- **Reflection & Review:** Mock Audit with Peer Review and AI Risk Mitigation Planning

FAQ:

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 AI technologies and data privacy laws 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 generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans five days, approximately 20-25 hours of instruction.

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

Auditing an AI system involves assessing performance, transparency, risk mitigation, and system trustworthiness throughout its lifecycle. Compliance checks merely verify if regulations are met. This course trains auditors to evaluate beyond regulatory checklists by integrating ethical AI assessments and emerging threat analysis.

How This Course is Different from Other AI Risk Management Courses:

Unlike traditional compliance-based AI training, this course emphasises *auditing intelligent systems across their entire lifecycle* using a multidimensional, governance-based framework. Drawing directly from the CSA publication "AI Risk Management: Thinking Beyond Regulatory Boundaries," it delivers practical tools such as audit question sets, ethical oversight strategies, and resilience assessments. Participants don’t just learn about AI risks; they practice identifying hidden vulnerabilities in AI infrastructure, data pipelines, and control systems through cutting-edge scenarios e.g., federated learning, fog computing, sensor abuse, and LLM audit methodologies. With a unique emphasis on human-in-the-loop governance, cloud system oversight, and privacy-enhancing technologies, the course transcends tick-box audits to empower professionals in shaping future-proof, legally defensible, and ethically sound AI environments.

AGILE LEADERS
Training Center

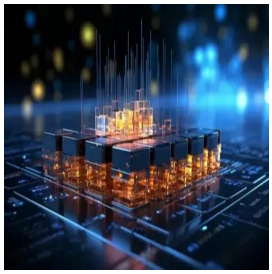
Training Course Categories

Finance and Accounting Training Courses

Agile PM and Project Management Training Courses

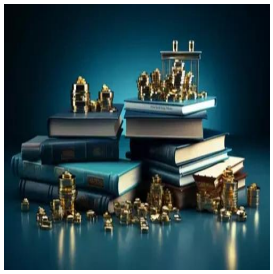
Certified Courses By International Bodies

Communication and Public Relations Training Courses



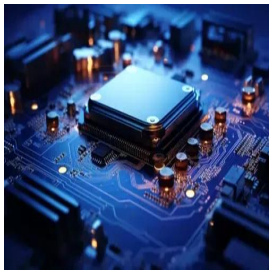
Data Analytics Training and Data Science Courses

Environment & Sustainability Training Courses



Governance, Risk and Compliance Training Courses

Human Resources Training and Development Courses



IT Security Training & IT Training Courses

Leadership and Management Training Courses

Legal Training, Procurement and Contracting Courses

Maintenance Training and Engineering Training Courses

AGILE LEADERS
Training Center

Training Course Categories

Marketing, Customer Relations, and Sales Courses

Occupational Health, Safety and Security Training Courses

Oil & Gas Training and Other Technical Courses

Personal & Self-Development Training Courses

Quality and Operations Management Training Courses

Secretarial and Administration Training Courses

AGILE LEADERS
Training Center

Training Cities

Accra - Ghana

Amman - Jordan

Amsterdam - Netherlands

Athens - Greece

Baku - Azerbaijan

Bali - Indonesia

Bangkok - Thailand

Barcelona - Spain

Cairo - Egypt

Cape town - South Africa

Casablanca - Morocco

Chicago - USA

Doha - Qatar

Dubai - UAE

Geneva - Switzerland

Istanbul - Turkey

AGILE LEADERS
Training Center

Training Cities

Jakarta - Indonesia

Johannesburg - South Africa

Kuala Lumpur - Malaysia

Langkawi - Malaysia

London - UK

Madrid - Spain

Manama - Bahrain

Milan - Italy

Montreux - Switzerland

Munich - Germany

Nairobi - Kenya

Paris - France

Phuket - Thailand

Prague - Czech Republic

Rome - Italy

San Diego - USA

Training Cities

Sharm El-Sheikh - Egypt

Tbilisi - Georgia

Tokyo - Japan

Trabzon - Turkey

Vienna - Austria

Zanzibar - Tanzania

Zoom - Online Training

WHO WE ARE

Agile Leaders is a renowned training center with a team of experienced experts in vocational training and development. With 20 years of industry experience, we are committed to helping executives and managers replace traditional practices with more effective and agile approaches.

OUR VISION

We aspire to be the top choice training provider for organizations seeking to embrace agile business practices. As we progress towards our vision, our focus becomes increasingly customer-centric and agile.

OUR MISSION

We are dedicated to developing value-adding, customer-centric agile training courses that deliver a clear return on investment. Guided by our core agile values, we ensure our training is actionable and impactful.

WHAT DO WE OFFER

At Agile Leaders, we offer agile, bite-sized training courses that provide a real-life return on investment. Our courses focus on enhancing knowledge, improving skills, and changing attitudes. We achieve this through engaging and interactive training techniques, including Q&As, live discussions, games, and puzzles.

AGILE LEADERS
Training Center

CONTACT US

UAE, Dubai Investment Park First

+971585964727
+447700176600

sales@agile4training.com