CORE CONCEPT

AI Governance, Risk and Compliance in Saudi Arabia: SDAIA AI Ethics Principles and Risk Framework

7 – 11 December 2026
London - Central London four-star

AI Governance, Risk and Compliance in Saudi Arabia: SDAIA AI Ethics Principles and Risk Framework

Ref: 1144_5948 **Date:** 7 – 11 December 2026 **Location:** London - Central London four-star **Fees:** 23000 SAR

Technical depth: Conceptual · **Practical mode:** Case study

Introduction

Organisations in Saudi Arabia are adopting AI faster than they are assigning accountability for it. SDAIA, the Saudi Data and AI Authority, now expects AI to follow its AI Ethics Principles and risk categories, and in 2026 issued a National AI Risk Management Framework, while the Personal Data Protection Law governs the data behind every model. Yet AI often sits between IT, risk, legal and data teams with no single framework. This Core Concept course equips senior leaders to direct governance built on SDAIA requirements and ISO/IEC 42001, ending with an AI Governance, Risk and Compliance Framework for their organisation.

Course Objectives

- Interpret the SDAIA AI Ethics Principles and risk categories and compare them with the OECD AI Principles and the UNESCO Recommendation
- Evaluate the organisation's AI governance maturity against the SDAIA AI Adoption Framework, ISO/IEC 42001 and the NIST AI RMF
- Direct the design of an AI governance operating model, policy architecture and decision rights
- Oversee AI risk, impact assessment and compliance obligations using the SDAIA National AI Risk Management Framework and PDPL requirements
- Judge the adequacy of controls for generative AI, deepfakes, bias, privacy, third-party supply and incident response
- Approve an AI Governance, Risk and Compliance Framework with an assurance plan across the three lines

Target Audience

- Chief risk officers and heads of enterprise risk responsible for emerging technology risk
- Chief compliance officers and heads of legal accountable for SDAIA, PDPL and sector regulatory obligations
- Chief data, digital and technology officers who own AI platforms and data assets
- Chief audit executives and heads of assurance who plan coverage of AI systems
- Members of AI governance, ethics and risk committees who approve AI use cases and policies

Course Outline

Day 1: The Case for AI Governance in Saudi Arabia and the Current State

- AI Governance Drivers: Regulatory, Ethical, Reputational and Operational
- SDAIA AI Ethics Principles: Seven Principles and Four Risk Categories
- SDAIA Principles Compared with the OECD AI Principles and UNESCO Recommendation
- AI Use Inventory and Risk-Level Classification
- AI Governance Maturity Assessment Against the SDAIA AI Adoption Framework and ISO/IEC 42001

Day 2: National and International Standards for AI Governance and Risk

- SDAIA National AI Risk Management Framework: Five-Stage Cycle and 4x4 Risk Matrix
- ISO/IEC 42001 AI Management System Requirements and Annex A Controls
- ISO/IEC 23894 and NIST AI RMF Functions Mapped to the SDAIA Framework
- ISO/IEC 42005 AI System Impact Assessment Process
- ISO 37301 Compliance Management System Applied to AI Obligations

Day 3: Designing the Governance, Risk and Compliance Architecture

- AI Governance Operating Model: Committee Structure, Roles and Decision Rights
- AI Policy Architecture: Acceptable Use, Procurement, Development and Monitoring
- AI Risk Register and Risk Appetite Thresholds
- AI Compliance Obligations Register: PDPL, NCA ECC-2:2024 and Sector Regulator Rules
- Principle-to-Control Mapping for the Seven SDAIA AI Ethics Principles

Day 4: High-Risk Areas and Control Gaps

- SDAIA Generative AI Guidelines and the NIST AI 600-1 Risk Profile
- SDAIA Deepfakes Guidelines and Synthetic Content Controls
- Bias and Fairness Oversight Using ISO/IEC TS 12791
- PDPL Cross-Border Transfer Rules and Privacy by Design under ISO/IEC 27701
- Third-Party AI Supplier Due Diligence, Contract Clauses and Incident Escalation

Day 5: Case Work and the AI GRC Framework

- Saudi Government Service Case Study: Automated Eligibility Decisions Under Challenge
- Saudi Banking Case Study: Governance Gaps in a Generative AI Assistant
- AI Governance, Risk and Compliance Framework Drafting for an Own Organisation
- Assurance Plan Using the Three Lines Model and Internal Audit Coverage
- Executive Panel Review and Framework Defence

Skills You Will Gain

- AI Governance Design
- AI Ethics Principles Application
- AI Risk Oversight
- AI Impact Assessment Review
- Compliance Obligations Management
- AI Policy Development
- Third-Party AI Risk Oversight
- AI Assurance Planning

Why Attend This Course

- Return to work with an AI Governance, Risk and Compliance Framework ready to table at your executive or governance committee
- Bring IT, risk, legal, data and audit onto one set of SDAIA-aligned standards, registers and decision rights for AI
- Recognise which AI uses fall into SDAIA's higher risk categories and need an impact assessment, stronger controls or escalation
- Compare governance approaches with senior leaders from Saudi government, banking, energy and healthcare organisations

Conclusion

AI governance works only when principles are turned into roles, registers, controls and assurance that someone owns. This course moves from the SDAIA AI Ethics Principles and the maturity of current practice, through SDAIA's National AI Risk Management Framework, ISO/IEC 42001, ISO/IEC 23894 and the NIST AI RMF, to the operating model, policies and controls for the highest-risk uses in Saudi Arabia. The final day turns that material into an AI Governance, Risk and Compliance Framework that participants take back to their executive team as the basis for accountable AI adoption.