AI Governance and Compliance Framework

Framework for Organisational Governance of AI Systems and Regulatory Compliance

IFAIS-GOV-001

Version 1.0 — 12 February 2025

Published by
International Federation for AI Standards (IFAIS)

Harmonised with ISO/IEC 42001, EU AI Act governance requirements, NIST AI RMF, OECD AI Principles, and sector-specific regulatory frameworks

Contents

Foreword

Advances in artificial intelligence have created new responsibilities for organisations deploying AI systems. AI governance and compliance are now foundational pillars for ensuring safe, accountable and transparent deployment across all sectors.

This IFAIS Governance Framework provides a structured, internationally harmonised set of requirements for:

- organisational accountability structures,
- compliance management and regulatory alignment,
- risk management processes,
- lifecycle documentation and auditability,
- incident response and monitoring,
- ethics, fairness and societal impact controls.

The framework is aligned with global regulatory trends and is intended for enterprises of all sizes.

Introduction

As AI systems become embedded in critical operations, organisations must adopt mature governance structures to ensure their systems are lawful, safe, trustworthy and aligned with human oversight requirements.

This framework addresses organisational-level controls, complementing technical standards such as IFAIS-IOP-001 and IFAIS-GSF-001. The scope includes roles, responsibilities, processes, documentation structures and compliance mechanisms.

Scope

This framework applies to all organisations that:

- design, develop or deploy AI systems,
- integrate third-party models or AI-powered services,
- operate AI within regulated markets (healthcare, finance, public sector, critical infrastructure),
- use AI for decision support or fully automated decision-making.

Out of scope: Component-level safety requirements (see IFAIS-GSF-001), technical interoperability (IFAIS-IOP-001), and ethical principles (IFAIS-ETH-001).

Normative References

- ISO/IEC 42001:2023 — AI Management System Standard (AIMS)
- EU AI Act (2024) — Governance, Transparency and High-Risk Obligations
- OECD Principles on Artificial Intelligence
- NIST AI Risk Management Framework (AI RMF)
- ISO/IEC 23894 — AI Risk Management
- IFAIS Safety Standard (IFAIS-GSF-001)
- IFAIS Interoperability Standard (IFAIS-IOP-001)

Terms and Definitions

AI Governance Organisational structures, processes and controls ensuring responsible development, deployment and oversight of AI systems.

Regulatory Compliance Conformance with applicable laws, standards, contractual obligations and sector-specific rules when using AI systems.

Risk Register Centralised record of identified risks, impact ratings, mitigation strategies and residual risks for each AI system.

Human Oversight Measures ensuring that humans can monitor, intervene in, or override AI system decisions when necessary.

Accountability Structure Clear allocation of responsibilities across senior leadership, AI risk officers, system owners and auditors.

Governance Structure

Senior Leadership Responsibilities

Executives must ensure:

- clear organisational AI governance policy,

- resourcing for compliance functions,
- assignment of roles and responsibilities,
- approval of high-risk AI deployments,
- periodic governance reviews.

AI Governance Committee

A cross-functional committee shall:

- oversee AI lifecycle governance,
- assess regulatory obligations,
- approve risk assessments,
- monitor incidents and post-deployment impacts,
- validate documentation completeness.

Roles and Responsibilities

Role	Primary Responsibilities
AI System Owner	Operational responsibility, documentation, monitoring
Data Protection Officer	Privacy impact assessments, legal compliance
AI Risk Officer	Risk assessments, mitigation tracking, audit readiness
Model Developer	Technical accuracy, robustness, reproducibility
Compliance Officer	Regulatory mapping, reporting, evidence collection
Audit Lead	Internal/external audit facilitation and verification

Compliance Management

Regulatory Mapping

Organisations shall document:

- all applicable AI-related regulations,
- jurisdiction-specific rules (EU, US, APAC),
- sectoral requirements (finance, health, transport),
- contractual obligations of models or datasets.

Compliance must be updated annually or when regulations change.

Policy Framework

Required policies include:

- AI Acceptable Use Policy,
- Data Governance Policy,
- Model Lifecycle Management Policy,

- Bias/Fairness Mitigation Policy,
- Third-Party Model Usage Policy,
- Incident Reporting Policy.

Evidence and Documentation

To demonstrate compliance, organisations must maintain:

- training data documentation,
- model cards and decision logs,
- risk assessments and mitigation summaries,
- human oversight procedures,
- changelogs and version histories.

AI Risk Management

Risk management must follow ISO/IEC 23894 and NIST AI RMF principles.

Risk Identification

Examples include:

- bias and discrimination,
- model drift and accuracy degradation,
- data poisoning or adversarial manipulation,
- security vulnerabilities,
- operational disruption or cascading failures.

Risk Assessment

Each risk must be rated by:

- impact,
- likelihood,
- detectability,
- residual risk after mitigation.

Risk Controls

Controls include:

- human-in-the-loop approval,
- explainability tooling,
- fairness testing pipelines,

- input/output filtering,
- continuous monitoring triggers.

Lifecycle Governance Requirements

Design Phase

- define intended purpose and limitations,
- conduct preliminary risk assessment,
- perform regulatory classification (e.g., EU high-risk),
- document data sources and licensing.

Development Phase

- maintain version control and reproducibility,
- apply fairness metrics and tests,
- ensure security and robustness testing,
- maintain dataset lineage and governance records.

Deployment Phase

- validate model performance on live data,
- ensure human oversight is implemented,
- approve system readiness via governance committee.

Post-Deployment Monitoring

- drift detection,
- anomaly detection,
- performance logs,
- error rate tracking,
- periodic re-assessment of regulatory classification.

Auditability and Transparency

Organisations must maintain audit trails covering:

- model versions and hashes,
- inference logs (privacy-preserving),
- decision rationales (where applicable),
- data access events,
- governance approvals,
- incident reports and resolutions.

External audits should occur at least once every 24 months.

Incident Response and Reporting

An AI-specific incident management process must include:

- incident detection and alerting,
- triage and severity classification,
- containment and rollback procedures,
- root cause analysis,
- mandatory reporting to regulators (where required),
- post-incident review and documentation.

Incidents include harmful outputs, security breaches, drift-induced failures, and regulatory non-conformance.

Third-Party AI and Procurement Controls

Organisations using external AI models must:

- conduct vendor risk assessments,
- validate training data provenance,
- review vendor compliance certifications,
- assess export format compatibility (e.g., ONNX),
- establish contractual audit rights.

Conformance Levels

Level 1 — Foundational Governance

- basic policies and documentation,
- identified compliance obligations.

Level 2 — Standard Governance

- full lifecycle governance,
- documented risk management,
- monitoring and audit trails.

Level 3 — Advanced Governance

- predictive monitoring,
- continuous risk re-evaluation,
- cross-system governance integration.

Implementation Guidance

- Templates for risk registers, DPIAs and model cards.
- Example governance workflows.
- Choosing appropriate oversight mechanisms (HITL, HOTL, HOOTL).
- Integrating governance with MLOps and DevOps pipelines.
- Communication strategies for stakeholders and regulators.

Sector-Specific Governance Profiles

Healthcare: Clinical validation, real-world evidence monitoring. **Finance:** Algorithmic fairness, anti-discrimination controls. **Public Sector:** Transparency and accessibility requirements. **Transport/AV:** Safety case documentation and scenario testing. **Defence:** Multi-layer oversight and classified assessments.